IBM Spectrum Protect for Linux 8.1.12

Installationshandbuch

Anmerkung:

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen” auf Seite 211 gelesen werden.

Impressum

Diese Ausgabe bezieht sich auf Version 8, Release 1, Modifikation 12 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.

Inhaltsverzeichnis

Inhalt dieser Veröffentlichung

Diese Veröffentlichung enthält Installations- und Konfigurationsanweisungen für den IBM Spectrum Protect-Server, die Serversprachen, die Lizenz und den Einheitentreiber.

Diese Veröffentlichung enthält außerdem Anweisungen zur Installation des Operations Center.

Zielgruppe

Diese Veröffentlichung richtet sich an Systemadministratoren, die den IBM Spectrum Protect-Server oder das Operations Center installieren, konfigurieren oder aktualisieren.

Installierbare Komponenten

Der IBM Spectrum Protect-Server und Lizenzen sind erforderliche Komponenten.

Diese Komponenten befinden sich in mehreren verschiedenen Installationspaketen.

Tabelle 1. Installierbare IBM Spectrum Protect-Komponenten

IBM Spectrum Protect-Komponente	**Beschreibung**	**Zusätzliche Informationen**
Server (erforderlich)	Enthält die Datenbank, Global Security Kit (GSKit), IBM® Java™ Runtime Environment (JRE) und Tools, die die Konfiguration und Verwaltung des Servers erleichtern.	„IBM Spectrum Protect mit dem Installationsassistenten installieren” auf Seite 84
Sprachenpaket (optional)	Jedes Sprachenpaket (eines pro Sprache) enthält sprachenspezifische Informationen für den Server.	Siehe „Serversprachenpakete installieren” auf Seite 86.
Lizenzen (erforderlich)	Enthält Unterstützung für alle lizenzierten Features. Nach der Installation dieses Pakets müssen Sie die erworbenen Lizenzen registrieren.	Verwenden Sie den Befehl **REGISTER LICENSE**.
Einheiten (optional)	Erweitert die Funktionalität der Datenträgerverwaltung.	Eine Liste der von diesem Treiber unterstützten Einheiten finden Sie im IBM Support Portal.

Tabelle 1. Installierbare IBM Spectrum Protect-Komponenten (Forts.)		
IBM Spectrum Protect-Komponente	**Beschreibung**	**Zusätzliche Informationen**
Speicheragent (optional)	Installiert die Komponente, mit der Clientsysteme Daten direkt auf Speichereinheiten, die an ein Speicherbereichsnetz (SAN) angeschlossen sind, schreiben können bzw. Daten direkt von dort lesen können. **Hinweis:** IBM Spectrum Protect for Storage Area Networks ist ein separates Lizenzprodukt.	Weitere Informationen zu Speicheragenten finden Sie in Tivoli Storage Manager for Storage Area Networks (Version 7.1.1).
Operations Center (optional)	Installiert das Operations Center, eine webbasierte Schnittstelle für die Verwaltung Ihrer Speicherumgebung.	Siehe Teil 2, „Operations Center installieren und Operations Center-Upgrade durchführen", auf Seite 133.

Veröffentlichungen

Die IBM Spectrum Protect-Produktfamilie umfasst IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, IBM Spectrum Protect for Databases und verschiedene andere Speicherverwaltungsprodukte von IBM.

Die IBM Produktdokumentation finden Sie unter IBM Knowledge Center.

Neuerungen in diesem Release

In diesem Release von IBM Spectrum Protect gibt es neue Funktionen und Aktualisierungen.

Eine Liste der neuen Funktionen und der Aktualisierungen finden Sie in Neuerungen.

Änderungen in der Dokumentation sind durch einen vertikalen Balken (|) am Seitenrand gekennzeichnet.

Teil 1. Server installieren und Upgrade durchführen

IBM Spectrum Protect-Server installieren und Upgrade des Servers durchführen.

Kapitel 1. Installation des Servers planen

Installieren Sie die Server-Software auf dem Computer, der Speichereinheiten verwaltet, und die Client-Software auf jeder Workstation, die Daten an den vom IBM Spectrum Protect-Server verwalteten Speicher überträgt.

Vorausgesetzte Kenntnisse

Sie müssen mit Ihren Betriebssystemen, Speichereinheiten, Übertragungsprotokollen und Systemkonfigurationen vertraut sein, bevor Sie IBM Spectrum Protect installieren.

Wartungsreleases, Client-Software und Veröffentlichungen für den Server stehen im IBM Support Portal zur Verfügung.

Einschränkung: Sie können den IBM Spectrum Protect-Server mit einigen Einschränkungen auf einem System installieren und ausführen, auf dem bereits IBM Db2 installiert ist. Das gilt unabhängig davon, ob Db2 separat oder als Teil einer anderen Anwendung installiert wurde.

Ausführliche Informationen siehe „Kompatibilität des IBM Spectrum Protect-Servers mit anderen IBM Db2-Produkten auf dem System" auf Seite 58.

Erfahrene Db2-Administratoren können erweiterte SQL-Abfragen durchführen und mithilfe von Db2-Tools die Datenbank überwachen. Sie dürfen die Db2-Tools jedoch nicht zur Änderung der von IBM Spectrum Protect vorgegebenen Db2-Konfigurationseinstellungen verwenden oder die Db2-Umgebung für IBM Spectrum Protect auf andere Weise ändern (z. B. mit anderen Produkten). Der Server wurde mit der Datendefinitionssprache (DDL) und der vom Server implementierten Datenbankkonfiguration erstellt und ausführlich getestet.

Achtung: Sie dürfen die Db2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der Db2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

Was Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten

Lesen Sie die Informationen zu den erweiterten Sicherheitsfunktionen im IBM Spectrum Protect-Server und den Anforderungen für die Aktualisierung Ihrer Umgebung.

Vorbereitende Schritte

Ab Version 8.1.2 wurden IBM Spectrum Protect Erweiterungen hinzugefügt, mit denen strengere Sicherheitseinstellungen durchgesetzt werden. Führen Sie vor der Installation oder dem Upgrade von IBM Spectrum Protect die folgenden Schritte aus:

- Lesen Sie im IBM Knowledge Center unter *Neuerungen* die Informationen in den Abschnitten 'Sicherheit' zu den Sicherheitsupdates für jede Version.
- Wenn Sie über Vorgängerversionen des Servers in Ihrer Umgebung verfügen, beachten Sie die Einschränkungen und bekannten Probleme in Technote 562939. Um diese Einschränkungen zu vermeiden und die neuesten Sicherheitserweiterungen zu nutzen, planen Sie für alle IBM Spectrum Protect-Server und -Clients für Sichern/Archivieren in Ihrer Umgebung eine Aktualisierung auf die neueste Version.

Sicherheitserweiterungen

Die folgenden Sicherheitserweiterungen wurden ab Version 8.1.2 hinzugefügt:

Sicherheitsprotokoll, das Transport Layer Security (TLS) verwendet

IBM Spectrum Protect Version 8.1.2 und spätere Software verfügt über ein verbessertes Sicherheitsprotokoll, das TLS Version 1.2 oder höher für die Authentifizierung zwischen dem Server, dem Speicheragenten und den Clients für Sichern/Archivieren verwendet.

Ab IBM Spectrum Protect Version 8.1.11 können Sie das TLS 1.3-Protokoll für die sichere Kommunikation zwischen Servern, Clients und Speicheragenten aktivieren. Damit TLS 1.3 verwendet werden kann, müssen beide Teilnehmer einer Kommunikationssitzung TLS 1.3 verwenden. Wenn einer der Teilnehmer TLS 1.2 verwendet, verwenden standardmäßig beide Teilnehmer TLS 1.2.

Automatische Secure Sockets Layer-Konfiguration (SSL-Konfiguration) und Verteilung von Zertifikaten

Server, Speicheragenten und Clients, die Software der Version 8.1.2 oder höher verwenden, werden automatisch für die gegenseitige Authentifizierung unter Verwendung von TLS konfiguriert.

Mit dem neuen Protokoll verfügt jeder Server, Speicheragent und Client über ein eindeutiges selbst signiertes Zertifikat, das für die Authentifizierung und für TLS-Verbindungen verwendet wird. Selbst signierte IBM Spectrum Protect-Zertifikate ermöglichen eine sichere Authentifizierung zwischen Entitäten, ermöglichen eine starke Verschlüsselung für die Datenübertragung und verteilen automatisch öffentliche Schlüssel an Clientknoten. Zertifikate werden automatisch zwischen allen Clients, Speicheragenten und Servern ausgetauscht, die Software der Version 8.1.2 oder höher verwenden. Sie müssen TLS nicht manuell konfigurieren oder die Zertifikate für jeden Client manuell installieren. Die neuen TLS-Erweiterungen erfordern keine Änderungen an den Optionen, und Zertifikate werden automatisch beim ersten Verbindungsaufbau auf Clients übertragen, sofern Sie nicht eine einzelne Administrator-ID für den Zugriff auf mehrere Systeme verwenden.

Standardmäßig werden selbst signierte Zertifikate verteilt. Sie können jedoch wahlweise andere Konfigurationen wie z. B. Zertifikate verwenden, die von einer Zertifizierungsstelle signiert werden. Weitere Informationen zur Verwendung von Zertifikaten finden Sie in *SSL- und TLS-Kommunikation* im IBM Knowledge Center.

Kombination von TCP/IP- und TLS-Protokollen für sichere Kommunikation und minimale Auswirkungen auf die Leistung

In Vorgängerversionen der IBM Spectrum Protect-Software mussten Sie entweder TLS oder TCP/IP für die Verschlüsselung der gesamten Kommunikation auswählen. Das neue Sicherheitsprotokoll verwendet eine Kombination von TCP/IP und TLS, um die Kommunikation zwischen Servern, Clients und Speicheragenten zu schützen. Standardmäßig wird TLS nur verwendet, um die Authentifizierung und die Metadaten zu verschlüsseln, während TCP/IP für die Datenübertragung verwendet wird. Da die TLS-Verschlüsselung primär nur für die Authentifizierung verwendet wird, ist die Leistung für Sicherungs- und Zurückschreibungsoperationen nicht betroffen.

Wahlweise können Sie TLS für die Verschlüsselung der Datenübertragung verwenden, indem Sie die Clientoption **SSL** für die Client/Server-Kommunikation und den Parameter **SSL** im Befehl **UPDATE SERVER** für die Kommunikation zwischen Servern verwenden.

Abwärtskompatibilität vereinfacht die Planung von Upgrades in Batches

Aktualisierte Versionen von IBM Spectrum Protect-Servern und -Clients können weiterhin eine Verbindung zu älteren Versionen herstellen, wenn der Parameter **SESSIONSECURITY** auf TRANSITIONAL gesetzt wird.

Sie müssen Clients für Sichern/Archivieren nicht auf Version 8.1.2 oder höher aktualisieren, bevor Sie ein Upgrade für Server durchführen. Nachdem Sie für einen Server ein Upgrade auf Version 8.1.2 oder höher durchgeführt haben, kommunizieren Knoten und Administratoren, die frühere Versionen der Software verwenden, weiterhin mit dem Server unter Verwendung des Werts TRANSITIONAL, bis die Entität die Anforderungen für den Wert STRICT erfüllt. Ähnlich können Sie für Clients für Sichern/Archivieren ein Upgrade auf Version 8.1.2 oder höher durchführen, bevor Sie ein Upgrade für Ihre IBM Spectrum Protect-Server durchführen, aber Sie müssen nicht erst für Server ein Upgrade durchführen. Die Kommunikation zwischen Servern und Clients, die verschiedene Versionen verwenden, wird nicht unterbrochen. Sie verfügen jedoch erst über die Vorteile der Sicherheitserweiterungen, wenn für Clients und Server ein Upgrade durchgeführt wurde.

Strenge Sicherheit mit dem Parameter SESSIONSECURITY durchsetzen

Um das neue Sicherheitsprotokoll zu verwenden, müssen die Server-, Clientknoten- oder Administratorentitäten IBM Spectrum Protect-Software verwenden, die den Parameter **SESSIONSECURITY** unterstützt. Sitzungssicherheit ist die Sicherheitsstufe, die für die Kommunikation zwischen IBM Spectrum Protect-Clientknoten, Verwaltungsclients und Servern verwendet wird. Sie können die folgenden Werte für diesen Parameter angeben:

STRICT
Setzt die höchste Sicherheitsstufe für die Kommunikation zwischen IBM Spectrum Protect-Servern, Knoten und Administratoren durch, die derzeit TLS 1.2 ist.

TRANSITIONAL
Gibt an, dass das vorhandene Kommunikationsprotokoll (z. B. TCP/IP) verwendet wird, bis Sie Ihre IBM Spectrum Protect-Software auf Version 8.1.2 oder höher aktualisieren. Dies ist der Standardwert. Bei **SESSIONSECURITY=TRANSITIONAL** werden strengere Sicherheitseinstellungen automatisch durchgesetzt, wenn höhere Versionen des TLS-Protokolls verwendet werden und die Software auf Version 8.1.2 oder höher aktualisiert wird. Wenn ein Knoten, Administrator oder Server die Anforderungen für den Wert STRICT erfüllt, wird die Sitzungssicherheit automatisch auf den Wert STRICT aktualisiert, und die Entität kann sich nicht mehr unter Verwendung einer Vorgängerversion des Clients oder früherer TLS-Protokolle authentifizieren.

Wenn **SESSIONSECURITY=TRANSITIONAL** angegeben ist und der Server, Knoten oder Administrator nie die Anforderungen für den Wert STRICT erfüllt hat, authentifiziert sich der Server, Knoten oder Administrator weiterhin unter Verwendung des Werts TRANSITIONAL. Wenn der Server, Knoten oder Administrator die Anforderungen für den Wert STRICT jedoch erfüllt, wird der Wert des Parameters **SESSIONSECURITY** automatisch von TRANSITIONAL in STRICT aktualisiert. Der Server, Knoten oder Administrator kann sich dann nicht mehr mit einer Version des Clients oder mit einem SSL/TLS-Protokoll authentifizieren, die bzw. das die Anforderungen für STRICT nicht erfüllt.

Einschränkung: Nachdem sich ein Administrator erfolgreich mithilfe von IBM Spectrum Protect-Software der Version 8.1.2 oder höher oder Tivoli Storage Manager-Software der Version 7.1.8 oder höher mit einem Server authentifiziert hat, kann sich der Administrator nicht mehr unter Verwendung von Client- oder Serverversionen vor Version 8.1.2 oder Version 7.1.8 mit demselben Server authentifizieren. Diese Einschränkung gilt auch für den Zielserver bei Verwendung von Funktionen wie z. B. Befehlsweiterleitung, Export zwischen Servern, die sich mit dem IBM Spectrum Protect-Zielserver als Administrator von einem anderen Server authentifizieren, Administratorverbindungen unter Verwendung des Operations Center und Verbindungen vom Verwaltungsbefehlszeilenclient.

Für Client- und Verwaltungssitzungen können Verwaltungsbefehlsweiterleitungssitzungen fehlschlagen, es sei denn, die Administrator-ID hat bereits Zertifikate für alle Server erworben, zu denen die Administrator-ID eine Verbindung herstellt. Administratoren, die sich mithilfe des Befehls **dsmadmc**, des Befehls **dsmc** oder des Programms dsm authentifizieren, können sich nicht unter Verwendung einer früheren Version authentifizieren, nachdem sie sich mit Version 8.1.2 oder höher authentifiziert haben. Lesen Sie die folgenden Tipps, um Authentifizierungsprobleme für Administratoren zu beheben:

- Stellen Sie sicher, dass für die gesamte IBM Spectrum Protect-Software, die vom Administratorkonto für die Anmeldung verwendet wird, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird. Wenn sich ein Administratorkonto von mehreren Systemen aus anmeldet, stellen Sie sicher, dass das Zertifikat des Servers auf allen Systemen installiert wird.
- Falls erforderlich, erstellen Sie ein separates Administratorkonto, das nur mit Clients und Servern verwendet werden soll, die Software der Version 8.1.1 oder früher verwenden.

Vor dem Upgrade

Bevor Sie ein Upgrade für einen Server durchführen, überprüfen Sie die Richtlinien in der folgenden Prüfliste.

Tabelle 2. Planungsprüfliste

Richtlinie	**Beschreibung**
Sichern Sie die folgenden Serverdateien: • Schlüsseldatenbanken (cert.kdb und dsmkeydb.kdb) • Stashdateien (cert.sth und dsmkeydb.sth)	Ab IBM Spectrum Protect Version 8.1.2 wird beim Start des Servers automatisch ein Masterverschlüsselungsschlüssel generiert, wenn der Masterverschlüsselungsschlüssel zuvor nicht vorhanden war. Der Masterverschlüsselungsschlüssel wird in einer Schlüsseldatenbank, dsmkeydb.kdb, gespeichert. Serverzertifikate werden weiterhin in der Schlüsseldatenbank 'cert.kdb' gespeichert. Der Zugriff erfolgt durch die Stashdatei 'cert.sth'. Sie müssen sowohl die Schlüsseldatenbanken (cert.kdb und dsmkeydb.kdb) als auch die Stashdateien (cert.sth und dsmkeydb.sth), die den Zugriff auf die jeweilige Schlüsseldatenbank bereitstellen, schützen. Standardmäßig schützt der Befehl **BACKUP DB** den Masterverschlüsselungsschlüssel auf dieselbe Art und Weise, auf der die Datenträgerprotokolldatei und die Datei devconfig geschützt werden. Sie müssen sich das Kennwort der Datenbanksicherung merken, um die Datenbank zurückzuschreiben. Die IBM Spectrum Protect-Serverdatei `dsmserv.pwd`, die in früheren Releases zum Speichern des Masterverschlüsselungsschlüssels verwendet wurde, wird nicht mehr verwendet.
Planen Sie sorgfältig Upgrades für Administrator-IDs	Identifizieren Sie alle Systeme, die von Administratorkonten verwendet werden, um sich für Verwaltungszwecke anzumelden. Nach einer erfolgreichen Authentifizierung mit Software der Version 8.1.2 oder höher können sich Administratoren nicht mit früheren Versionen von IBM Spectrum Protect-Software auf demselben Server authentifizieren. Wenn eine einzelne Administrator-ID für die Anmeldung bei mehreren Systemen verwendet wird, planen Sie für alle diese Systeme ein Upgrade mit Software der Version 8.1.2 oder höher, um sicherzustellen, dass das Zertifikat auf allen Systemen installiert wird, bei denen sich der Administrator anmeldet. **Tipp:** Sie werden nicht für einen Server gesperrt, wenn der Parameter **SESSIONSECURITY** für alle Ihre Administrator-IDs in den Wert STRICT aktualisiert wird. Sie können das öffentliche Serverzertifikat manuell in einen Client importieren, von dem der Befehl **dsmadmc** ausgegeben wird.

Tabelle 2. Planungsprüfliste (Forts.)

Richtlinie	Beschreibung
Wenn Sie TLS mit Vorgängerversionen des Clients verwenden, die das Zertifikat "TSM Server SelfSigned Key" (cert.arm) verwenden, aktualisieren Sie Ihre Clients auf Version 8.1.4 oder höher.	In Releases vor Version 7.1.8 hatte das Standardzertifikat den Kennsatz "TSM Server SelfSigned Key" und eine MD5-Signatur, die das TLS 1.2-Protokoll oder höher nicht unterstützt, das für Clients mit Version 8.1.2 oder höheren Versionen und für das Operations Center standardmäßig erforderlich ist. Führen Sie einen der folgenden Schritte aus, um dieses Problem zu beheben: • Führen Sie für den Server ein Upgrade auf Version 8.1.4 oder höher durch. Ab Version 8.1.4 werden Server, die das MD5-signierte Zertifikat als Standardwert verwenden, automatisch so aktualisiert, dass sie ein Standardzertifikat mit einer SHA-Signatur verwenden, die den Kennsatz "TSM Server SelfSigned SHA Key" hat. Eine Kopie des neuen Standardzertifikats wird in der Datei `cert256.arm` gespeichert, die sich im Serverinstanzverzeichnis befindet. **Tipp:** Bevor Sie den Server aktualisieren, um das neue Standardzertifikat mit einer SHA-Signatur zu verwenden, müssen Sie die Datei `cert256.arm` an Clients verteilen, damit keine Clientsicherungsfehler auftreten. Jeder Client muss das neue Zertifikat abrufen und importieren, bevor er eine Verbindung zu einem Server herstellen kann, der das neue SHA-Standardzertifikat verwendet. Es ist nicht erforderlich, vorherige Zertifikate zu entfernen. • Um das Standardzertifikat manuell zu aktualisieren, führen Sie die Anweisungen in Technote 562939 aus.

Nächste Schritte

- Befolgen Sie die Prozedur in „Sicherheitsupdates anwenden” auf Seite 7, um einen IBM Spectrum Protect-Server zu installieren oder ein Upgrade für einen Server durchzuführen.
- Informationen zur Behebung von Kommunikationsproblemen in Bezug auf Sicherheitsupdates finden Sie in „Fehlerbehebung für Sicherheitsupdates” auf Seite 14.
- FAQ-Informationen finden Sie in FAQ - Security updates in IBM Spectrum Protect.
- Informationen zur Verwendung des IBM Spectrum Protect-Web-Clients für Sichern/Archivieren in der neuen Sicherheitsumgebung finden Sie in Technote 728037.

Sicherheitsupdates anwenden

Wenden Sie Sicherheitsupdates an, die mit neuen Releases von IBM Spectrum Protect bereitgestellt werden.

Vorbereitende Schritte

Lesen Sie die folgenden Informationen:

- Details zu den mit einem Release bereitgestellten Sicherheitsupdates finden Sie im Abschnitt *Neuerungen* im IBM Knowledge Center.
- Informationen zu den Aktualisierungen und allen Einschränkungen, die zutreffen können, finden Sie in „Was Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten" auf Seite 3.
- Um die Reihenfolge zu bestimmen, in der ein Upgrade für die Server und Clients in Ihrer Umgebung durchgeführt wird, beantworten Sie die folgenden Fragen:

Tabelle 3. Fragen, die vor dem Upgrade zu beachten sind

Frage	**Hinweis**
Welche Rolle hat der Server in der Konfiguration?	Im Allgemeinen können Sie zunächst ein Upgrade für die IBM Spectrum Protect-Server in Ihrer Umgebung und dann ein Upgrade für Clients für Sichern/Archivieren durchführen. Unter bestimmten Umständen (z. B. bei Verwendung von Funktionen für die Befehlsweiterleitung) kann der Server jedoch als Client in Ihrer Konfiguration agieren. Um Kommunikationsprobleme zu verhindern, wird in diesem Fall empfohlen, zunächst ein Upgrade für Clients durchzuführen. Informationen zu verschiedenen Szenarios finden Sie in Upgradeszenarios.

Tabelle 3. Fragen, die vor dem Upgrade zu beachten sind (Forts.)

Frage	Hinweis
Welche Systeme werden für die Administratorauthentifizierung verwendet?	Für Administratorkonten ist die Reihenfolge wichtig, in der ein Upgrade durchgeführt wird, um Authentifizierungsprobleme zu verhindern. – Für Clients auf mehreren Systemen, die sich mit derselben ID anmelden (Knoten- oder Administrator-ID), muss gleichzeitig ein Upgrade durchgeführt werden. Serverzertifikate werden bei der ersten Verbindung automatisch auf Clients übertragen. – Bevor Sie ein Upgrade für Ihren Server durchführen, beachten Sie alle Endpunkte, die der Administrator für Verwaltungszwecke für die Herstellung der Verbindung verwendet. Wenn eine einzelne Administrator-ID für den Zugriff auf mehrere Systeme verwendet wird, stellen Sie sicher, dass das Zertifikat des Servers auf allen Systemen installiert wird. – Nachdem sich eine Administrator-ID erfolgreich mithilfe von IBM Spectrum Protect-Software der Version 8.1.2 oder höher oder Tivoli Storage Manager-Software der Version 7.1.8 oder höher mit dem Server authentifiziert hat, kann sich der Administrator nicht mehr unter Verwendung von Client- oder Serverversionen vor Version 8.1.2 oder Version 7.1.8 mit diesem Server authentifizieren. Dies gilt auch für einen Zielserver, wenn Sie sich mit diesem IBM Spectrum Protect-Zielserver als Administrator von einem anderen Server authentifizieren. Dies gilt beispielsweise bei Verwendung der folgenden Funktionen: - Befehlsweiterleitung - Export zwischen Servern - Herstellen der Verbindung von einem Verwaltungsclient im Operations Center

Tabelle 3. Fragen, die vor dem Upgrade zu beachten sind (Forts.)

Frage	**Hinweis**
In welcher Reihenfolge sollte das Upgrade für meine Systeme erfolgen?	– **Wenn Sie ein Upgrade für Server durchführen, bevor Sie ein Upgrade für Clientknoten durchführen:** - Führen Sie zunächst ein Upgrade für den Hub-Server und dann für alle Peripherieserver durch. - Wenn Sie für einen Server ein Upgrade auf Version 8.1.2 oder höher durchführen, können Knoten und Administratoren, die frühere Versionen der Software verwenden, weiterhin mit dem neuen Server unter Verwendung des vorhandenen Kommunikationsprotokolls kommunizieren. Wenn **SESSIONSECURITY** auf TRANSITIONAL gesetzt wird und der Server, Knoten oder Administrator nie die Anforderungen für den Wert STRICT erfüllt hat, authentifiziert sich der Server, Knoten oder Administrator weiterhin unter Verwendung des Werts TRANSITIONAL. Wenn der Server, Knoten oder Administrator die Anforderungen für den Wert STRICT jedoch erfüllt, wird der Wert des Parameters **SESSIONSECURITY** automatisch von TRANSITIONAL in STRICT aktualisiert. – **Wenn Sie ein Upgrade für Clientknoten durchführen, bevor Sie ein Upgrade für Server durchführen:** - Führen Sie zunächst ein Upgrade für Verwaltungsclients und dann für Nicht-Verwaltungsclients durch. Clients mit höheren Release-Level kommunizieren weiterhin mit Servern mit früheren Versionen. **Wichtig:** Wenn Sie für einen der Verwaltungsclients in Ihrer Umgebung ein Upgrade durchführen, muss für alle anderen Clients, die dieselbe ID wie der aktualisierte Client verwenden, gleichzeitig ein Upgrade durchgeführt werden. - Es ist nicht erforderlich, für alle Nicht-Verwaltungsclients gleichzeitig ein Upgrade durchzuführen, es sei denn, mehrere Clients verwenden dieselbe ID für die Anmeldung. In diesem Fall muss für alle anderen Clients, die dieselbe ID wie der aktualisierte Client verwenden, gleichzeitig ein Upgrade durchgeführt werden und das Zertifikat des Servers muss auf allen Systemen installiert werden.

Informationen zu diesem Vorgang

Enthält Ihre Umgebung IBM Spectrum Protect-Clients für Sichern/Archivieren oder IBM Spectrum Protect-Server mit einer Version vor Version 7.1.8 oder Version 8.1.2, müssen Sie möglicherweise Ihre Konfiguration anpassen, um sicherzustellen, dass die Kommunikation zwischen Servern und Clients nicht unterbrochen wird. Befolgen Sie die in diesem Abschnitt beschriebene Standardprozedur für die Installation oder das Upgrade Ihrer Umgebung.

Überprüfen Sie Upgradeszenarios auf andere Beispielszenarios, die möglicherweise auf Ihre Umgebung zutreffen.

Tipp: Um die neuesten Sicherheitserweiterungen zu nutzen, planen Sie für alle IBM Spectrum Protect-Server und -Clients für Sichern/Archivieren in Ihrer Umgebung eine Aktualisierung auf den neuesten Release-Level.

Vorgehensweise

1. Installieren Sie IBM Spectrum Protect-Server in Ihrer Umgebung oder führen Sie ein Upgrade für die Server durch. Weitere Informationen finden Sie in dem Abschnitt *Server installieren und Upgrade für den Server durchführen* im IBM Knowledge Center.
   a) Führen Sie ein Upgrade für das Operations Center und den Hub-Server durch. Weitere Informationen finden Sie in Teil 2, „Operations Center installieren und Operations Center-Upgrade durchführen", auf Seite 133.
   b) Führen Sie ein Upgrade für Peripherieserver durch.
   c) Konfigurieren oder verifizieren Sie die Kommunikation zwischen Servern. Weitere Informationen finden Sie in:
      - Befehl *UPDATE SERVER* im IBM Knowledge Center.
      - Abschnitt *SSL-Kommunikation zwischen dem Hub-Server und einem Peripherieserver konfigurieren* im IBM Knowledge Center.
      - Abschnitt *Server für die Verbindung zu einem anderen Server unter Verwendung von SSL konfigurieren* im IBM Knowledge Center.

      Tipp:

      - Ab IBM Spectrum Protect Version 8.1.2 und Tivoli Storage Manager Version 7.1.8 verwendet der Parameter **SSL** SSL, um die Kommunikation mit dem angegebenen Server zu verschlüsseln, auch wenn der Parameter **SSL** auf NO gesetzt ist.
      - Ab Version 8.1.4 werden Zertifikate zwischen Speicheragenten, Speicherarchivclients und Speicherarchivmanager-Servern automatisch konfiguriert. Zertifikate werden ausgetauscht, wenn zum ersten Mal eine serverübergreifende Verbindung zu einem Server mit erweiterter Sicherheit hergestellt wird.
2. Installieren Sie Verwaltungsclients oder führen Sie ein Upgrade für Verwaltungsclients durch. Weitere Informationen finden Sie in dem Abschnitt *Clients installieren und konfigurieren* im IBM Knowledge Center.
3. Aktivieren Sie die sichere Kommunikation zwischen allen Systemen, die von Administratoren verwendet werden, um sich für Verwaltungszwecke anzumelden.
   - Stellen Sie sicher, dass für die IBM Spectrum Protect-Software, die vom Administratorkonto für die Anmeldung verwendet wird, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird.
   - Wenn sich eine Administrator-ID von mehreren Systemen aus anmeldet, stellen Sie sicher, dass das Zertifikat des Servers auf allen Systemen installiert wird.
4. Installieren Sie Nicht-Verwaltungsclients oder führen Sie ein Upgrade für Nicht-Verwaltungsclients durch. Weitere Informationen finden Sie in dem Abschnitt *Clients installieren und konfigurieren* im IBM Knowledge Center.

   Hinweis: Sie können für Ihre Nicht-Verwaltungsclients stufenweise ein Upgrade durchführen. Sie können weiterhin eine Verbindung zu Servern mit höheren Release-Level von Clients mit früheren Re-

lease-Level herstellen, indem Sie den Befehl **UPDATE NODE** ausgeben und den Parameter **SESSIONS-ECURITY** für jeden Knoten auf TRANSITIONAL setzen.

```
update node Knotenname sessionsecurity=transitional
```

Nächste Schritte

Möglicherweise treffen andere Upgradeszenarios auf Ihre Umgebung zu. Überprüfen Sie die Beispielupgradeszenarios in der folgenden Tabelle.

Tabelle 4. Upgradeszenarios

Szenario	Hinweise	Vorgeschlagene Upgrademethode
Funktionen für die Verwaltungsbefehlsweiterleitung werden verwendet, um Befehle an einen oder mehrere Server weiterzuleiten. Es soll eine Verbindung zu einem IBM Spectrum Protect-Server mit einer Version vor Version 8.1.2 hergestellt werden.	• Bei der Befehlsweiterleitung kann der Server als Verwaltungsclient agieren. • Die Befehlsweiterleitung verwendet die ID und das Kennwort des Administrators, der den Befehl ausgibt. • Wenn Sie eine einzelne Administrator-ID für den Zugriff auf mehrere Systeme verwenden, stellen Sie sicher, dass das Zertifikat des Servers auf allen Systemen installiert wird.	• Führen Sie zunächst ein Upgrade für den Verwaltungsclient durch. **Wichtig:** Für Clients auf mehreren Systemen, die sich mit derselben Knoten- oder Administrator-ID anmelden, muss gleichzeitig ein Upgrade durchgeführt werden. • Stellen Sie auf jedem Server, an den Befehle weitergeleitet werden, sicher, dass die folgenden Informationen konfiguriert werden: – Dieselbe Administrator-ID und dasselbe Kennwort – Die erforderliche Administratorberechtigung auf jedem Server – Die erforderlichen Zertifikate • Führen Sie für die Server, die vom Administratorkonto für die Anmeldung verwendet werden, ein Upgrade auf Version 8.1.2 oder höher durch.

Tabelle 4. Upgradeszenarios (Forts.)

Szenario	Hinweise	Vorgeschlagene Upgrademethode
Der Verwaltungsclient verfügt über die neueste Releaseversion und es wird dieselbe Administrator-ID für die Authentifizierung bei verschiedenen Systemen mithilfe des Befehls **dsmadmc** verwendet. Die Authentifizierung bei einem IBM Spectrum Protect-Server in meiner Umgebung, der mit der neuesten Version ausgeführt wird, war erfolgreich. Jetzt soll die Authentifizierung bei einem Server mit einer Version vor Version 8.1.2 erfolgen.	• Nachdem sich ein Administrator bei einem IBM Spectrum Protect-Server der Version 8.1.2 oder höher mithilfe eines Clients der Version 8.1.2 oder höher authentifiziert hat, kann sich die Administrator-ID nur auf Clients oder Servern, die Version 8.1.2 oder höher verwenden, mit diesem Server authentifizieren. • Wenn Sie eine einzelne Administrator-ID für den Zugriff auf mehrere Systeme verwenden, planen Sie für alle diese Systeme ein Upgrade mit Software der Version 8.1.2 oder höher, um sicherzustellen, dass das Zertifikat des Servers auf allen Systemen installiert wird, bei denen sich der Administrator anmeldet.	• Stellen Sie sicher, dass für die gesamte IBM Spectrum Protect-Software, die von den Administratoren für die Anmeldung verwendet wird, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird. Die bevorzugte Aktion ist ein Upgrade für alle Server in Ihrer Umgebung auf die neueste Version. • Falls erforderlich, erstellen Sie ein separates Administratorkonto, das nur mit Clients und Servern verwendet werden soll, die Software der Version 8.1.1 oder früher verwenden.
Für den IBM Spectrum Protect-Server wurde bereits ein Upgrade auf den neuesten Release-Level durchgeführt. Es ist ein Verwaltungsclient mit dem Release-Level 8.1.0 vorhanden und es soll eine Verbindung zum Server vom Operations Center hergestellt werden.	• Wenn Sie für einen der Verwaltungsclients in Ihrer Umgebung ein Upgrade durchführen, muss für alle anderen Clients, die dieselbe ID wie der aktualisierte Client verwenden, gleichzeitig ein Upgrade durchgeführt werden. • Um eine Administrator-ID in einer Konfiguration mit mehreren Servern zu verwenden, muss die ID auf dem Hub-Server und den Peripherieservern mit demselben Kennwort, derselben Berechtigungsstufe und den erforderlichen Zertifikaten registriert werden.	• Überprüfen Sie auf jedem Server, ob die folgenden Informationen definiert sind: – Dieselbe Administrator-ID und dasselbe Kennwort – Die erforderliche Administratorberechtigung auf jedem Server – Die erforderlichen Zertifikate • Führen Sie für Nicht-Verwaltungsclients stufenweise ein Upgrade durch.
Die Knotenreplikation wird zum Schutz der Daten verwendet.	• Der Replikationsheartbeat leitet einen Zertifikatsaustausch ein, wenn die erste serverübergreifende Verbindung hergestellt wird, nachdem für den Server ein Upgrade durchgeführt wurde.	• Führen Sie für Ihre Server ein Upgrade durch, bevor Sie für Ihre Clients ein Upgrade durchführen; befolgen Sie die Standardprozedur.

Tabelle 4. Upgradeszenarios (Forts.)

Szenario	Hinweise	Vorgeschlagene Upgrademethode
Vor dem Upgrade der Server soll ein Upgrade für die Clients für Sichern/Archivieren durchgeführt werden.	• Nachdem Sie für einen Server ein Upgrade auf Version 8.1.2 oder höher durchgeführt haben, kommunizieren Knoten und Administratoren, die frühere Versionen der Software verwenden, weiterhin mit dem Server unter Verwendung des Werts TRANSITIONAL, bis die Entität die Anforderungen für den Wert STRICT erfüllt. • Die Kommunikation zwischen Servern und Clients wird nicht unterbrochen.	• Wenn Sie ein Upgrade für Ihre Clients durchführen, bevor Sie ein Upgrade für Ihre Server durchführen, führen Sie zunächst ein Upgrade für Verwaltungsclients und dann für Nicht-Verwaltungsclients durch. Clients mit höheren Release-Level kommunizieren weiterhin mit Servern mit früheren Versionen.

Fehlerbehebung für Sicherheitsupdates

Beheben Sie Probleme, die nach einem Upgrade für IBM Spectrum Protect auftreten können.

Symptom	Problemlösung
Ein Administratorkonto kann sich nicht bei einem System anmelden, das Software vor Version 8.1.2 verwendet.	Nachdem sich ein Administrator erfolgreich mithilfe von IBM Spectrum Protect-Software der Version 8.1.2 oder höher mit dem Server authentifiziert hat, kann sich der Administrator nicht mehr mit diesem Server authentifizieren, der Client- oder Serverversionen vor Version 8.1.2 verwendet. Diese Einschränkung gilt auch für den Zielserver bei Verwendung von Funktionen wie z. B. Befehlsweiterleitung, Export zwischen Servern, die sich mit dem IBM Spectrum Protect-Zielserver als Administrator von einem anderen Server authentifizieren, Administratorverbindungen, die das Operations Center verwenden, und Verbindungen vom Verwaltungsbefehlszeilenclient. Führen Sie die folgenden Schritte aus, um Authentifizierungsprobleme für Administratoren zu beheben: 1. Identifizieren Sie alle Systeme, von denen sich Administratoren anmelden und die die Administrator-ID für die Anmeldung verwenden. Führen Sie für die Systemsoftware ein Upgrade auf IBM Spectrum Protect Version 8.1.2 oder höher durch und stellen Sie sicher, dass das Zertifikat des Servers auf allen Systemen installiert wird. 2. Setzen Sie den Wert des Parameters **SESSIONSECURITY** für den Administrator auf TRANSITIONAL, indem Sie den Befehl `update admin *Administratorname* sessionsecurity=transitional` ausgeben. 3. Wiederholen Sie die Administratorverbindung. **Tipp:** Falls erforderlich, erstellen Sie ein separates Administratorkonto, das nur mit Clients und Servern verwendet werden soll, die Software der Version 8.1.1 oder früher verwenden.
Verteilung von Zertifikaten ist für einen Knoten, Administrator oder Server fehlgeschlagen.	Ein Knoten, Administrator oder Server, der Software der Version 8.1.2 oder höher verwendet, hat den Wert STRICT für **SESSIONSECURITY**, aber der Wert muss auf TRANSITIONAL zurückgesetzt werden, um die Verteilung von Zertifikaten zu wiederholen. Wenn das neue Protokoll verwendet wird, wird die automatische Übertragung eines öffentlichen Serverzertifikats nur bei der ersten Verbindung zu einem

Symptom	Problemlösung

	Server mit erweiterter Sicherheit ausgeführt. Nach der ersten Verbindung ändert sich der Wert des Parameters **SESSIONSECURITY** für einen Knoten von TRANSITIONAL in STRICT. Sie können einen Knoten, Administrator oder Server vorübergehend in TRANSITIONAL aktualisieren, um eine andere automatische Übertragung des Zertifikats zu ermöglichen. Während der Wert TRANSITIONAL aktiv ist, überträgt die nächste Verbindung bei Bedarf automatisch das Zertifikat und setzt den Parameter **SESSIONSECURITY** auf STRICT zurück.
	
	Aktualisieren Sie den Wert des Parameters **SESSIONSECURITY** in TRANSITIONAL, indem Sie einen der folgenden Befehle ausgeben:
	
	• Geben Sie für Clientknoten Folgendes aus:
	`update node` *`Knotenname`* `sessionsecurity=transitional`
	• Geben Sie für Administratoren Folgendes aus:
	`update admin` *`Administratorname`* `sessionsecurity=transitional`
	• Geben Sie für Server Folgendes aus:
	`update server` *`Servername`* `sessionsecurity=transitional`
	
	Alternativ können Sie das öffentliche Zertifikat manuell übertragen und importieren, indem Sie mit dem Dienstprogramm 'dsmcert' die folgenden Befehle ausgeben:
	
	`openssl s_client -connect tapsrv04:1500 -showcerts > tapsrv04.arm`
	
	`dsmcert -add -server tapsrv04 -file tapsrv04.arm`
	
	Wenn Sie CA-signierte Zertifikate verwenden, müssen Sie das CA-Stammzertifikat und alle CA-Zwischenzertifikate in jeder Schlüsseldatenbank für den Client, Server und Speicheragenten installieren, der eine SSL-Kommunikation einleitet.

Zertifikatsaustausch zwischen IBM Spectrum Protect-Servern war nicht erfolgreich.	Wenn das neue Protokoll verwendet wird, wird die automatische Übertragung eines öffentlichen Serverzertifikats nur bei der ersten Verbindung zu einem Server mit erweiterter Sicherheit ausgeführt. Nach der ersten Verbindung ändert sich der Wert des Parameters **SESSIONSECURITY** für einen Server von TRANSITIONAL in STRICT. Wiederholen Sie den Zertifikatsaustausch zwischen zwei IBM Spectrum Protect-Servern. Informationen finden Sie in *Zertifikatsaustausch zwischen Servern wiederholen*.
Zertifikatsaustausch zwischen einem IBM Spectrum Protect-Server und einem Clientknoten war nicht erfolgreich.	Wenn das neue Protokoll verwendet wird, wird die automatische Übertragung eines öffentlichen Serverzertifikats nur bei der ersten Verbindung zu einem Server mit erweiterter Sicherheit ausgeführt. Nach der ersten Verbindung ändert sich der Wert des Parameters **SESSIONSECURITY** für einen Knoten von TRANSITIONAL in STRICT. Führen Sie die folgenden Schritte aus, um den Zertifikatsaustausch zwischen Clients und Servern einer Version vor Version 8.1.2 zu wiederholen: 1. Rekonfigurieren Sie vorhandene Clients, die für die Verwendung von SSL mit dem Zertifikat 'cert.arm' konfiguriert sind, für die Verwendung des Zertifikats `cert256.arm`. Anweisungen finden Sie in *Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren* im IBM Knowledge Center. 2. Aktualisieren Sie das Standardzertifikat, indem Sie den folgenden Befehl im Serverinstanzverzeichnis ausgeben: `gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed -label "TSM Server SelfSigned SHA Key"`

Symptom	Problemlösung

	3. Starten Sie den Server erneut.
	
	Für Clients und Server der Version 8.1.2 und höher werden die Zertifikate automatisch verteilt. Wenn die Kommunikation zwischen Clients oder Servern fehlschlägt, führen Sie die folgenden Schritte aus, um die Verteilung von Zertifikaten zu wiederholen:
	
	1. Setzen Sie für Knoten und Administratoren den Parameter **SESSIONSECURITY** auf TRANSITIONAL, indem Sie die folgenden Befehle für jeden gewünschten Knoten oder Administrator ausgeben:
	
	`update node` *`Knotenname`* `sessionsecurity=transitional`
	`update admin` *`Administratorname`* `sessionsecurity=transitional`
	
	Tipp: Administratoren, die sich mithilfe des Befehls **dsmadmc**, des Befehls **dsmc** oder des Programms dsm authentifizieren, können sich nicht unter Verwendung einer früheren Version authentifizieren, nachdem sie sich mit Version 8.1.2 oder höher authentifiziert haben. Lesen Sie die folgenden Tipps, um Authentifizierungsprobleme für Administratoren zu beheben:
	
	• Stellen Sie sicher, dass für die gesamte IBM Spectrum Protect-Software, die vom Administratorkonto für die Anmeldung verwendet wird, ein Upgrade auf Version 8.1.2 oder höher durchgeführt wird. Wenn sich ein Administratorkonto von mehreren Systemen aus anmeldet, stellen Sie sicher, dass das Zertifikat des Servers auf allen Systemen installiert wird, bevor das Administratorkonto für die Befehlsweiterleitung verwendet wird.
	
	• Nachdem sich ein Administrator bei einem Server der Version 8.1.2 oder höher mithilfe eines Clients der Version 8.1.2 oder höher authentifiziert hat, kann sich der Administrator nur auf Clients oder Servern authentifizieren, die Version 8.1.2 oder höher verwenden. Ein Administratorbefehl kann von jedem System ausgegeben werden. Falls erforderlich, erstellen Sie ein separates Administratorkonto, das nur mit Clients und Servern verwendet werden soll, die Software der Version 8.1.1 oder früher verwenden.
	
	2. Aktualisieren Sie für Speicheragenten die Option **STASESSIONSECURITY** in der Speicheragentenoptionsdatei `dsmsta.opt`, indem Sie den Wert STRICT in TRANSITIONAL ändern.
	
	3. Starten Sie die Server erneut. Zertifikatsänderungen werden erst nach dem Neustart der Server oder Speicheragenten wirksam.
	
	4. Können Zertifikate nach der Ausführung der Schritte 1 bis 4 immer noch nicht ausgetauscht werden, fügen Sie den Servern und Speicheragenten die Zertifikate manuell hinzu und starten Sie die Server und Speicheragenten erneut. Anweisungen finden Sie in *Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren* im IBM Knowledge Center.

Zertifikate sollen manuell an Clientsysteme verteilt werden.	Der IBM Spectrum Protect-Serveradministrator kann einen Client für Sichern/Archivieren automatisch implementieren, um Workstations zu aktualisieren, auf denen der Client für Sichern/Archivieren bereits installiert ist. Informationen finden Sie in *Automatische Implementierung des Clients für Sichern/Archivieren* im IBM Knowledge Center. Lesen Sie die Informationen in *IBM Spectrum Protect-Client/Server-Kommunikation mit Secure Sockets Layer konfigurieren* im IBM Knowledge Center.
Zertifikate für Sitzungen zwischen Clients	Das Dienstprogramm 'dsmcert', das mit dem IBM Spectrum Protect-Client für Sichern/Archivieren installiert wird, wird verwendet, um einen Zertifikatsspei-

Symptom	Problemlösung
sollen zurückgesetzt werden.	cher für Serverzertifikate zu erstellen. Verwenden Sie das Dienstprogramm 'dsmcert', um die Dateien zu löschen und die Zertifikate erneut zu importieren.
Als Rootbenutzer wollen Sie Benutzern ohne Rootberechtigung die Verwaltung Ihrer Dateien erlauben.	Der Trusted Communication Agent (TCA), der bisher von Benutzern ohne Rootberechtigung in IBM Spectrum Protect-Clients der Version 8.1.0, 7.1.6 und früheren Versionen verwendet wurde, ist nicht mehr verfügbar. Rootbenutzer können Benutzern ohne Rootberechtigung die Verwaltung ihrer Dateien mit den folgenden Methoden ermöglichen: **Help-Desk** Bei der Help-Desk-Methode führt der Rootbenutzer alle Sicherungs- und Zurückschreibungsoperationen aus. Der Benutzer ohne Rootberechtigung muss sich an den Rootbenutzer wenden, um die Sicherung oder Zurückschreibung bestimmter Dateien anzufordern. **Berechtigter Benutzer** Bei der Methode mit einem berechtigten Benutzer erhält ein Benutzer ohne Rootberechtigung Schreib-/Lesezugriff auf den Kennwortspeicher. Hierbei wird die Option `passworddir` verwendet, um auf eine Kennwortposition zu zeigen, auf die der Benutzer ohne Rootberechtigung Schreib-/Lesezugriff hat. Mit dieser Methode können Benutzer ohne Rootberechtigung ihre eigenen Dateien sichern und zurückschreiben, die Verschlüsselung verwenden und ihre eigenen Kennwörter mit der Option `passwordaccess generate` verwalten. Weitere Informationen finden Sie in *Benutzern ohne Rootberechtigung die Verwaltung eigener Daten ermöglichen* im IBM Knowledge Center. Ist keine dieser Methoden zufriedenstellend, müssen Sie die früheren Clients verwenden, die über den Trusted Communication Agent (TCA) verfügen.
Sie wollen GSKit-Kompatibilitätsprobleme lösen.	Sind auf einem System mehrere Anwendungen installiert, die GSKit verwenden, können Inkompatibilitätsprobleme auftreten. Lesen Sie die folgenden Informationen, um diese Probleme zu lösen: • Technote 2011742 für IBM Spectrum Protect-Clients. • Technote 7050721 für Db2. • Technote 2007298 für IBM Spectrum Protect-Server. • Technote 7050721 für IBM Spectrum Protect-Server und -Clients auf demselben Windows-System.

Weitere Informationen zur Fehlerbehebung bei Sicherheitsupdates finden Sie in Technote 2004844.

Zertifikatsaustausch zwischen Servern wiederholen

Wenn der Zertifikatsaustausch zwischen Servern fehlschlägt, können Sie den Austausch wiederholen.

Vorgehensweise

1. Entfernen Sie das Zertifikat aus der Datenbank des Partnerservers, indem Sie den folgenden Befehl auf beiden Servern ausgeben:

   ```
   update server Servername forcesync=yes
   ```

   Tipp: Der Server verwendet möglicherweise das falsche Zertifikat, wenn Sie immer noch Fehlernachrichten für jede serverübergreifende Sitzung empfangen, nachdem Sie die Schritte in dieser Task ausgeführt und die Server erneut gestartet haben. Wenn Sie feststellen, dass der Server versucht, das fal-

sche Zertifikat zu verwenden, löschen Sie das Zertifikat aus der Schlüsseldatenbank, indem Sie den folgenden Befehl ausgeben:

```
gsk8capicmd_64 -cert -delete -db cert.kdb -stashed -label Zertifikatskennsatz
```

2. Löschen Sie die Serverdefinition, indem Sie den Befehl **DELETE SERVER** für den Server und den Partnerserver ausgeben. Wenn Sie die Serverdefinition nicht löschen können, müssen Sie die Zertifikate manuell konfigurieren. Anweisungen zum manuellen Konfigurieren von Zertifikaten finden Sie in *Speicheragenten, Server, Clients und das Operations Center für die Verbindung zum Server unter Verwendung von SSL konfigurieren* im IBM Knowledge Center.
3. Um das Zertifikat wieder zu erwerben, konfigurieren Sie die Server mithilfe der Überkreuzdefinition und ermöglichen Sie den Servern den Austausch von Zertifikaten, indem Sie die folgenden Befehle auf beiden Servern ausgeben:

```
set crossdefine on
set serverhladdress Adresse_der_höheren_Ebene
set serverlladdress Adresse_der_unteren_Ebene
set serverpassword Kennwort
```

4. Geben Sie den folgenden Befehl auf einem der Server aus, die mithilfe der Überkreuzdefinition konfiguriert werden:

```
define server Servername crossdefine=yes ssl=yes
```

5. Wiederholen Sie Schritt 3 für alle anderen Serverpaare der Version 8.1.2 oder höher.
6. Starten Sie die Server erneut.
7. Um sicherzustellen, dass Zertifikate ausgetauscht wurden, geben Sie den folgenden Befehl im Serverinstanzverzeichnis jedes Servers aus, der überprüft werden soll:

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

Beispielausgabe:

```
example.website.com:1542:0
```

Tipp: Bei Verwendung der Replikation wird der Replikationsheartbeat ungefähr alle 5 Minuten ausgeführt, und leitet einen Zertifikatsaustausch ein, wenn die erste Verbindung hergestellt wird, nachdem für den Server ein Upgrade durchgeführt wurde. Diese Verbindung hat zur Folge, dass die Nachrichten ANR8583E und ANR8599W einmal in dem Protokoll angezeigt werden, bevor ein Zertifikatsaustausch stattfindet. Wird die Replikation nicht verwendet, werden Zertifikate ausgetauscht, wenn zum ersten Mal eine serverübergreifende Sitzung eingeleitet wird, außer für Serverkonfigurationen ohne einen auf beiden Computern definierten Server.

8. Für Server, die als virtueller Datenträger definiert sind, führen Sie die folgenden Schritte aus:
   a) Entfernen Sie das Partnerzertifikat aus der Serverdatenbank, indem Sie den folgenden Befehl auf beiden Servern ausgeben:

```
update server Servername forcesync=yes
```

   b) Stellen Sie sicher, dass für den Serverkennwortwert im Befehl **DEFINE SERVER** auf dem Quellenserver, den Kennwortwert im Befehl **REGISTER NODE** auf dem als virtueller Datenträger definierten Server und den Wert für **SET SERVERPASSWORD** auf dem als virtueller Datenträger definierten Server dasselbe Kennwort verwendet wird. Falls erforderlich, aktualisieren Sie ein Kennwort mithilfe des Befehls **UPDATE SERVER**, **UPDATE NODE** bzw. **SET SERVERPASSWORD**. Zertifikate werden nach der ersten Clientsicherung von dem als virtueller Datenträger definierten Server auf dem Quellenserver ausgetauscht.
9. Können Zertifikate immer noch nicht zwischen Servern ausgetauscht werden, führen Sie die folgenden Schritte aus:
   a) Stellen Sie in der Serverdefinition für jeden kommunizierenden Server sicher, dass ein Servername angegeben wurde, der mit dem Namen übereinstimmt, der durch die Ausgabe des Befehls **SET SERVERNAME** auf dem Partnerserver definiert wurde.

b) Stellen Sie sicher, dass Serverdefinitionen über Kennwörter verfügen, die mit dem Befehl **SET SERVERPASSWORD** definiert wurden. Die Kennwörter müssen mit dem Wert übereinstimmen, der mit dem Befehl **SET SERVERNAME** für den Partnerserver angegeben wird.

c) Geben Sie nach der Ausführung der Schritte a und b den folgenden Befehl erneut aus:

```
update server Servername forcesync=yes
```

d) Wiederholen Sie die Schritte 1 bis 3.

Planung für optimale Leistung

Überprüfen Sie vor der Installation des IBM Spectrum Protect-Servers die Merkmale und die Konfiguration des Systems, um sicherzustellen, dass der Server für die optimale Leistung konfiguriert ist.

Informationen zu diesem Vorgang

Die optimale IBM Spectrum Protect-Umgebung wird mithilfe der IBM Spectrum Protect Blueprints konfiguriert.

Vorgehensweise

1. Lesen Sie den Abschnitt „Vorausgesetzte Kenntnisse” auf Seite 3.
2. Lesen Sie jeden der folgenden Unterabschnitte.

Planung für die Server-Hardware und das Betriebssystem

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Werden die Betriebssystem- und Hardwarevoraussetzungen erfüllt oder mehr als erfüllt? • Anzahl und Geschwindigkeit der Prozessoren • Systemspeicher • Unterstützte Betriebssystemversion	Wenn Sie die erforderliche Mindestspeicherkapazität verwenden, können Sie eine minimale Arbeitslast unterstützen. Sie können versuchsweise mehr Systemspeicher hinzufügen, um bestimmen zu können, ob sich die Leistung verbessert. Entscheiden Sie dann, ob der Systemspeicher dem Server zugeordnet bleiben soll. Testen Sie die verschiedenen Speicherkapazitäten jeweils anhand des gesamten Tageszyklus der Serverlast. Wenn Sie mehrere Server auf dem System ausführen, addieren Sie die Voraussetzungen für jeden Server, um die Voraussetzungen für das System zu bestimmen.	Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 84861. Lesen Sie außerdem die Anweisungen in Tasks für Betriebssysteme und andere Anwendungen optimieren. Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten: • Prüfliste für Datendeduplizierung • Prüfliste für Knotenreplikation Weitere Informationen zu Anforderungen in Bezug auf die Größe des Servers und des Speichers finden Sie in den IBM Spectrum Protect Blueprints.
Sind Platten für die optimale Leistung konfiguriert?	Der Umfang der Optimierung, der für verschiedene Plattensysteme erfolgen kann, variiert. Stellen Sie sicher, dass die Warteschlangenlänge und andere Plattensystemoptionen entsprechend definiert sind.	Weitere Informationen finden Sie in: • "Planung für Platten für die Serverdatenbank" • "Planung für Platten für das Serverwiederherstellungsprotokoll" • "Planung für Speicherpools auf DISK- oder FILE-Einheiten"

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verfügt der Server über genügend Speicher?	Höhere Arbeitslasten und erweiterte Funktionen wie beispielsweise Datendeduplizierung und Knotenreplikation erfordern mehr Systemspeicher als den Mindestspeicher, der im Dokument mit den Systemvoraussetzungen angegeben ist. Verwenden Sie die folgenden Richtlinien, um den Speicherbedarf für Datenbanken anzugeben, die nicht für die Datendeduplizierung aktiviert sind: • Für Datenbanken mit einer Größe unter 500 GB benötigen Sie 16 GB Speicher. • Für Datenbanken mit einer Größe von 500 GB bis 1 TB benötigen Sie 24 GB Speicher. • Für Datenbanken mit einer Größe von 1 TB bis 1,5 TB benötigen Sie 32 GB Speicher. • Für Datenbanken mit einer Größe über 1,5 TB benötigen Sie 40 GB Speicher. Stellen Sie sicher, dass Sie für die Replikationsverarbeitung zusätzlichen Speicherbereich für die aktive Protokolldatei und das Archivprotokoll zuordnen.	Weitere Informationen zu Voraussetzungen, wenn die entsprechenden Funktionen verwendet werden, finden Sie in den folgenden Abschnitten: • Prüfliste für Datendeduplizierung • Prüfliste für Knotenreplikation • Speicherbedarf

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verfügt das System über genügend Hostbusadapter (HBAs), um die Datenoperationen, die der IBM Spectrum Protect-Server gleichzeitig ausführen muss, handhaben zu können?	Sie müssen wissen, für welche Operationen die gleichzeitige Verwendung von Hostbusadaptern erforderlich ist. Ein Server muss beispielsweise Sicherungsdaten mit 1 GB/s speichern, während er gleichzeitig eine Speicherpoolumlagerung ausführt, für deren Ausführung eine Kapazität von 0,5 GB/s erforderlich ist. Die Hostbusadapter müssen alle Daten mit der erforderlichen Geschwindigkeit handhaben können.	Siehe HBA-Kapazität optimieren.
Ist die Netzbandbreite größer als der geplante maximale Durchsatz für Sicherungen?	Die Netzbandbreite muss dem System die Ausführung von Operationen wie Sicherungen innerhalb der zulässigen Zeit oder gemäß den vereinbarten Service-Levels ermöglichen. Bei der Knotenreplikation muss die Netzbandbreite größer als der geplante maximale Durchsatz sein.	Weitere Informationen finden Sie in: • Netzleistung optimieren • Prüfliste für Knotenreplikation

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verwenden Sie ein bevorzugtes Dateisystem für IBM Spectrum Protect-Serverdateien?	Verwenden Sie ein Dateisystem, das optimale Leistung und Datenverfügbarkeit gewährleistet. Der Server verwendet die direkte E/A mit Dateisystemen, die die Funktion unterstützen. Die Verwendung der direkten E/A kann den Durchsatz verbessern und die Prozessornutzung verringern. Weitere Informationen zum bevorzugten Dateisystem für Ihr Betriebssystem finden Sie in IBM Spectrum Protect server-supported file systems.	Weitere Informationen finden Sie in Betriebssystem für die Plattenleistung konfigurieren.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Planen Sie, genügend Seitenauslagerungsbereich zu konfigurieren?	Seitenauslagerungsbereich (oder Auslagerungsspeicher) erweitert den Speicher, der für die Verarbeitung verfügbar ist. Wenn der freie Arbeitsspeicher im System knapp wird, werden Programme oder Daten, die nicht im Gebrauch sind, aus dem Speicher in den Seitenauslagerungsbereich versetzt. Mit dieser Aktion wird Speicherbereich für andere Aktivitäten, wie z. B. Datenbankoperationen, freigegeben. **Einschränkung:** Verwenden Sie keinen Seitenauslagerungsbereich, um Ihrem System Speicher hinzuzufügen. Der Seitenauslagerungsbereich soll lediglich eine begrenzte und vorübergehende Speichererweiterung bereitstellen. Wenn Ihr System Seitenauslagerungsbereich verwendet, ist der Systemspeicher voll und muss vergrößert werden. Verwenden Sie den größeren der beiden folgenden Werte: mindestens 32 GB Seitenauslagerungsbereich oder 50 % des Arbeitsspeichers.	
Planen Sie, nach der Installation des Servers die Kernelparameter zu optimieren?	Sie müssen Kernelparameter optimieren.	Informationen zur Optimierung von Kernelparametern finden Sie in Linux®: Kernelparameter für Linux-Systeme optimieren.

Planung für Platten für die Serverdatenbank

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Befindet sich die Datenbank auf schnellen Platten mit kurzer Latenzzeit?	Verwenden Sie die folgenden Laufwerke nicht für die IBM Spectrum Protect-Datenbank: • Nearline SAS (NL-SAS) • Serial Advanced Technology Attachment (SATA) • Parallel Advanced Technology Attachment (PATA) Verwenden Sie keine internen Platten, die standardmäßig Teil der Hardware der meisten Server ist. Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung. Wenn Sie planen, die Datendeduplizierungsfunktionen von IBM Spectrum Protect zu verwenden, legen Sie den Schwerpunkt auf die Plattenleistung (gemessen in E/A-Operationen pro Sekunde).	Weitere Informationen finden Sie in Prüfliste für Datendeduplizierung.
Ist die Datenbank auf anderen Platten oder LUNs gespeichert als die aktive Protokolldatei, das Archivprotokoll und die Speicherpooldatenträger?	Das Trennen der Serverdatenbank von anderen Serverkomponenten trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei. **Tipp:** Die Datenbank und das Archivprotokoll können ein Array gemeinsam nutzen, wenn Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) verwenden.	
Wissen Sie bei Verwendung von RAID, wie die optimale RAID-Stufe für Ihr System ausgewählt wird? Definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ?	Wenn ein System viele Schreibvorgänge ausführen muss, ist die Leistung bei RAID 10 besser als bei RAID 5. RAID 10 benötigt jedoch mehr Platten als RAID 5, um dieselbe nutzbare Speichermenge bereitzustellen. Handelt es sich bei Ihrem Plattensystem um ein RAID-System, definieren Sie alle LUNs mit derselben Größe und demselben RAID-Typ. Verwenden Sie beispielsweise nicht gleichzeitig 4+1 RAID 5 mit 4+2 RAID 6.	

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Planen Sie, wenn eine Option zum Definieren der Stripgröße oder der Segmentgröße verfügbar ist, die Größe beim Konfigurieren des Plattensystems zu optimieren?	Wenn Sie die Stripgröße oder Segmentgröße definieren können, verwenden Sie auf Plattensystemen für die Datenbank Größen von 64 KB oder 128 KB.	Die Blockgröße, die für die Datenbank verwendet wird, variiert abhängig vom Tabellenbereich. Die meisten Tabellenbereiche verwenden 8-KB-Blöcke; einige verwenden jedoch 32-KB-Blöcke.
Planen Sie, mindestens vier Verzeichnisse, die auch als Speicherpfade bezeichnet werden, auf vier verschiedenen LUNs für die Datenbank zu erstellen? Erstellen Sie exakt ein Verzeichnis pro Array in dem Subsystem. Wenn weniger als drei Arrays vorhanden sind, erstellen Sie in jedem Array einen anderen LUN-Datenträger.	Für größere Arbeitslasten und bei Verwendung einiger Funktionen sind mehr Datenbankspeicherpfade als die Mindestvoraussetzungen erforderlich. Serveroperationen wie die Datendeduplizierung verursachen eine hohe Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS) für die Datenbank. Die Leistung derartiger Operationen ist besser, wenn die Datenbank über mehr Verzeichnisse verfügt. Verwenden Sie für Serverdatenbanken, die größer als 2 TB sind oder die wahrscheinlich auf diese Größe anwachsen, acht Verzeichnisse. Berücksichtigen Sie das geplante Wachstum des Systems bei der Bestimmung der Anzahl zu erstellender Speicherpfade. Die höhere Anzahl Speicherpfade wird vom Server effizienter genutzt, wenn die Speicherpfade bei der Ersterstellung des Servers bereits vorhanden sind. Verwenden Sie die Variable *DB2_PARALLEL_IO*, um die parallele E/A für Tabellenbereiche mit einem einzelnen Container zu erzwingen oder für Tabellenbereiche, die über Container auf mehr als einer physischen Platte verfügen. Wenn Sie die Variable *DB2_PARALLEL_IO* nicht definieren, entspricht die E/A-Parallelität der Anzahl Container, die von dem Tabellenbereich verwendet werden. Wenn ein Tabellenbereich beispielsweise vier Container umfasst, beträgt der verwendete Grad an E/A-Parallelität 4.	Weitere Informationen finden Sie in: • Prüfliste für Datendeduplizierung • Prüfliste für Knotenreplikation Hilfreiche Informationen zur Vorhersage des Wachstums beim Deduplizieren von Daten durch den Server finden Sie in Technote 1596944. Aktuelle Informationen zur Datenbankgröße, zur Datenbankreorganisation und zu Leistungsaspekten für IBM Spectrum Protect-Server finden Sie in Technote 1683633. Informationen zum Definieren der Variable *DB2_PARALLEL_IO* finden Sie in Empfohlene Einstellungen für IBM Db2-Registry-Variablen.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben alle Verzeichnisse für die Datenbank dieselbe Größe?	Verzeichnisse, die alle dieselbe Größe haben, stellen einen konsistenten Grad an Parallelität für Datenbankoperationen sicher. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als andere sind, verringert sich dadurch das Potenzial für den optimierten parallelen Vorablesezugriff. Diese Richtlinie gilt auch, wenn Sie nach der Erstkonfiguration des Servers Speicherpfade hinzufügen müssen.	
Planen Sie, die Warteschlangenlänge der Datenbank-LUNs auf AIX-Systemen zu erhöhen?	Die Warteschlangenlänge ist häufig zu niedrig definiert.	Siehe AIX-Systeme für die Plattenleistung konfigurieren.

Planung für Platten für das Serverwiederherstellungsprotokoll

Überprüfen Sie mithilfe der Prüfliste, ob das System, auf dem der Server installiert ist, die Voraussetzungen in Bezug auf die Hardware- und Softwarekonfiguration erfüllt.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Sind die aktive Protokolldatei und das Archivprotokoll auf anderen Platten oder LUNs gespeichert als die Datenbank und die Speicherpooldatenträger?	Stellen Sie sicher, dass die Platten, auf die die aktive Protokolldatei gestellt wird, auf dem Server oder System nicht für andere Zwecke verwendet werden. Stellen Sie die aktive Protokolldatei nicht auf Platten, die die Serverdatenbank, das Archivprotokoll oder Systemdateien, wie Seitenauslagerungsbereich oder Auslagerungsspeicher, enthalten.	Das Trennen der Serverdatenbank von der aktiven Protokolldatei und dem Archivprotokoll trägt zur Reduktion von Konkurrenzsituationen für dieselben Ressourcen durch unterschiedliche Operationen, die gleichzeitig ausgeführt werden müssen, bei.
Befinden sich die Protokolle auf Platten mit nicht flüchtigem Schreibcache?	Nicht flüchtiger Schreibcache ermöglicht es, Daten so schnell wie möglich in die Protokolle zu schreiben. Schnellere Schreiboperationen für die Protokolle können die Leistung für Serveroperationen verbessern.	

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Legen Sie für die Protokolle eine Größe fest, die der Arbeitslast entspricht?	Wenn Sie sich über die Arbeitslast im Unklaren sind, verwenden Sie die größtmögliche Größe. **Aktive Protokolldatei** Die maximale Größe beträgt 512 GB; sie wird über die Serveroption **ACTIVELOGSIZE** festgelegt. Stellen Sie sicher, dass mindestens 8 GB freier Speicherbereich im Dateisystem für aktive Protokolldateien verfügbar sind, nachdem die aktiven Protokolldateien mit fester Größe erstellt wurden. **Archivprotokoll** Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Das Archivprotokoll muss mindestens so groß wie die aktive Protokolldatei sein.	• Ausführliche Informationen zur Festlegung der Protokollgröße enthalten die Informationen zum Wiederherstellungsprotokoll in Technote 400357. • Informationen zur Festlegung der Größe bei Verwendung der Datendeduplizierung finden Sie in Prüfliste für Datendeduplizierung.
Definieren Sie ein Archivübernahmeprotokoll? Stellen Sie dieses Protokoll auf eine andere Platte als das Archivprotokoll?	Das Archivübernahmeprotokoll dient der Verwendung durch den Server im Notfall, wenn das Archivprotokoll voll ist. Für das Archivübernahmeprotokoll können langsamere Platten verwendet werden.	Geben Sie die Position des Archivübernahmeprotokolls mithilfe der Serveroption **ARCHFAILOVERLOGDIRECTORY** an. Überwachen Sie die Belegung des Verzeichnisses für das Archivübernahmeprotokoll. Wenn das Archivübernahmeprotokoll vom Server verwendet werden muss, ist der Speicherplatz für das Archivprotokoll möglicherweise nicht groß genug.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verwenden Sie, wenn Sie die aktive Protokolldatei spiegeln, nur einen einzigen Typ von Spiegelung?	Sie können das Protokoll mithilfe einer der folgenden Methoden spiegeln. Verwenden Sie für das Protokoll nur einen einzigen Typ von Spiegelung. • Verwenden Sie die Option **MIRRORLOGDIRECTORY**, die für den IBM Spectrum Protect-Server verfügbar ist, um eine Position für die Spiegelung anzugeben. • Verwenden Sie die Softwarespiegelung, wie z. B. Logical Volume Manager (LVM) unter AIX. • Verwenden Sie die Spiegelung in der Hardware des Plattensystems.	Stellen Sie, wenn Sie die aktive Protokolldatei spiegeln, sicher, dass die Platten für die aktive Protokolldatei und die Spiegelkopie dieselbe Geschwindigkeit und Zuverlässigkeit haben. Weitere Informationen finden Sie in Wiederherstellungsprotokoll konfigurieren und optimieren.

Planung für Verzeichniscontainerspeicherpools und Cloud-Containerspeicherpools

Überprüfen Sie die Konfiguration Ihrer Verzeichniscontainer- und Cloud-Containerspeicherpools, um eine optimale Leistung zu gewährleisten.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verwenden Sie, gemessen in Anzahl Ein-/Ausgabeoperationen pro Sekunde (IOPS), schnellen Plattenspeicher für die IBM Spectrum Protect-Datenbank?	Verwenden Sie eine Hochleistungsplatte für die Datenbank. Verwenden Sie die Solid-State-Laufwerk-Technologie (SSD-Technologie) für die Datendeduplizierungsverarbeitung. Stellen Sie sicher, dass die Datenbank über eine Mindestkapazität von 3000 E/A-Operationen pro Sekunde (IOPS) verfügt. Addieren Sie zu diesem Mindestwert pro TB Daten, die täglich (vor der Datendeduplizierung) gesichert werden, 1000 E/A-Operationen pro Sekunde. Beispielsweise würde ein IBM Spectrum Protect-Server, der täglich 3 TB Daten aufnimmt, 6000 E/A-Operationen pro Sekunde (IOPS) für die Datenbankplatten benötigen: `mindestens 3000 IOPS + 3000 (3 TB x 1000 IOPS) = 6000 IOPS`	Empfehlungen zur Plattenauswahl finden Sie in "Planung für Platten für die Serverdatenbank". Weitere Informationen zu IOPS finden Sie in den IBM Spectrum Protect Blueprints.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Ist genügend Speicherplatz für die Größe Ihrer Datenbank vorhanden?	Verwenden Sie mindestens 40 GB Systemspeicher für IBM Spectrum Protect-Server, die Daten deduplizieren, mit einer Datenbankgröße von 100 GB. Wenn die Speicherkapazität für Sicherungsdaten wächst, ist unter Umständen ein höherer Speicherbedarf erforderlich. Überwachen Sie regelmäßig die Speicherbelegung, um festzustellen, ob mehr Speicherplatz erforderlich ist. Verwenden Sie weiteren Systemspeicher, um das Caching von Datenbankseiten zu verbessern. Die folgenden Richtlinien für die Speichergröße basieren auf dem Volumen an neuen Daten, das jeden Tag gesichert wird: • 128 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 1 und 2 TB liegt • 192 GB Systemspeicher für tägliche Sicherungen von Daten, wobei die Datenbankgröße zwischen 2 und 4 TB liegt	Speicherbedarf

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie die Speicherkapazität für die die aktive Protokolldatei und das Archivprotokoll der Datenbank korrekt festgelegt?	Geben Sie in der Konfiguration des Servers eine minimale Größe von 128 GB für die aktive Protokolldatei an, indem Sie die Serveroption **ACTIVELOGSIZE** auf den Wert 131072 setzen. Als Anfangsgröße für das Archivprotokoll wird eine Größe von 1 TB vorgeschlagen. Die Größe des Archivprotokolls wird durch die Größe des Dateisystems begrenzt, in dem es sich befindet, und nicht durch eine Serveroption. Stellen Sie sicher, dass im Vergleich zur Größe des Archivprotokolls mindestens 10 % zusätzlicher Plattenspeicher für das Dateisystem vorhanden sind. Verwenden Sie für die Datenbankarchivprotokolle ein Verzeichnis mit einer anfänglichen freien Kapazität von mindestens 1 TB. Geben Sie das Verzeichnis mithilfe der Serveroption **ARCHLOGDIRECTORY** an. Definieren Sie Speicherbereich für das Archivübernahmeprotokoll mithilfe der Serveroption **ARCHFAILOVERLOGDIRECTORY**.	Weitere Informationen zur Kapazitätsermittlung für Ihr System finden Sie in den IBM Spectrum Protect Blueprints.
Ist die Komprimierung für die Archivprotokoll- und Datenbanksicherungen aktiviert?	Aktivieren Sie die Serveroption ARCHLOGCOMPRESS, um Speicherbereich einzusparen. Diese Komprimierungsoption unterscheidet sich von der Inline-Komprimierung. Die Inline-Komprimierung ist ab IBM Spectrum Protect Version 7.1.5 und höher standardmäßig aktiviert. **Einschränkung:** Sie dürfen diese Option nicht verwenden, wenn das Volumen der pro Tag gesicherten Daten 6 TB überschreitet.	Weitere Informationen zur Komprimierung für Ihr System finden Sie in den IBM Spectrum Protect Blueprints.
Befinden sich die Datenbank und Protokolle von IBM Spectrum Protect auf separaten Plattendatenträgern (LUNs)? Ist der Datenträger, der für die Datenbank verwendet wird, gemäß den bewährten Verfahren für eine transaktionsorientierte Datenbank konfiguriert?	Die Datenbank darf keine Plattendatenträger mit IBM Spectrum Protect-Datenbankprotokollen oder -Speicherpools oder mit einer anderen Anwendung oder einem anderen Dateisystem gemeinsam nutzen.	Weitere Informationen zur Konfiguration der Serverdatenbank und des Wiederherstellungsprotokolls finden Sie in Konfiguration und Optimierung der Serverdatenbank und des Wiederherstellungsprotokolls.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Verwenden Sie mindestens acht Prozessorkerne (2,2-GHz-Prozessorkerne oder entsprechende Prozessorkerne) für jeden IBM Spectrum Protect-Server, der mit Datendeduplizierung verwendet werden soll?	Wenn die clientseitige Datendeduplizierung verwendet werden soll, müssen Sie sicherstellen, dass für Clientsysteme während einer Sicherungsoperation genügend Ressourcen zur Ausführung der Datendeduplizierungsverarbeitung verfügbar sind. Verwenden Sie pro Sicherungsprozess mit clientseitiger Datendeduplizierung einen Prozessor, der mindestens einem 2,2-GHz-Prozessorkern entspricht.	• Häufig gestellte Fragen zur Datendeduplizierung • IBM Spectrum Protect Blueprints
Haben Sie genügend Speicherplatz für die Datenbank zugeordnet?	Als grobe Schätzung sollten Sie 100 GB Datenbankspeicher für jeweils 25 TB Daten einplanen, die in deduplizierten Speicherpools geschützt werden sollen. *Geschützte Daten* ist das Datenvolumen vor der Datendeduplizierung, einschließlich aller Versionen gespeicherter Objekte. Für Datenbanksicherungsoperationen mit sehr vielen kleinen Dateien (durchschnittliche Dateigröße kleiner als 512 KB) benötigen Sie mehr Datenbankspeicherbereich. Planen Sie für kleinere Objektgrößen 100 GB Datenbankspeicherbereich für jeweils 10 TB Speicher ein. Als bewährtes Verfahren sollten Sie einen neuen Containerspeicherpool ausschließlich für die Datendeduplizierung definieren. Die Datendeduplizierung erfolgt auf der Speicherpoolebene; mit Ausnahme von verschlüsselten Daten werden alle Daten in einem Speicherpool dedupliziert.	Die optimale IBM Spectrum Protect-Umgebung wird mithilfe der IBM Spectrum Protect-Blueprints konfiguriert.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie die Speicherpoolkapazität geschätzt, um genügend Speicherplatz für die Größe Ihrer Umgebung zu konfigurieren?	Sie können den Kapazitätsbedarf für einen deduplizierten Speicherpool wie folgt schätzen: 1. Schätzen Sie die Basisgröße der Quellendaten. 2. Schätzen Sie die Größe der täglichen Sicherung anhand einer geschätzten Änderungs- und Wachstumsrate. 3. Bestimmen Sie die Anforderungen in Bezug auf die Aufbewahrungsdauer. 4. Schätzen Sie das Gesamtvolumen an Quellendaten unter Berücksichtigung der Basisgröße, der Größe der täglichen Sicherung und der Anforderungen in Bezug auf die Aufbewahrungsdauer. 5. Wenden Sie den Faktor für das Deduplizierungsverhältnis an. 6. Wenden Sie den Faktor für das Komprimierungsverhältnis an. 7. Runden Sie die Schätzung auf, um die Nutzung transienter Speicherpools zu berücksichtigen.	Ein Beispiel zur Verwendung dieses Verfahrens finden Sie in Häufig gestellte Fragen zur Datendeduplizierung.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie die Platten-E/A auf viele Platteneinheiten und Controller verteilt?	Verwenden Sie Arrays, die aus so vielen Platten wie möglich bestehen; dies wird auch als "Wide-Striping" bezeichnet. Stellen Sie sicher, dass Sie exakt ein Datenbankverzeichnis pro Array in dem Subsystem verwenden. Definieren Sie die Registry-Variable *DB2_PARALLEL_IO*, um die parallele E/A für jeden verwendeten Tabellenbereich zu aktivieren, wenn sich die Container in dem Tabellenbereich über mehrere physische Platten erstrecken. Wenn E/A-Bandbreite verfügbar ist und die Dateien groß sind (beispielsweise 1 MB), kann der Prozess zur Suche nach Duplikaten die Ressourcen eines gesamten Prozessors in Anspruch nehmen. Wenn Dateien kleiner sind, können andere Engpässe auftreten. Geben Sie acht oder mehr Dateisysteme für die Einheitenklasse des deduplizierten Speicherpools an, damit die Ein-/Ausgabe auf so viele LUNs und physische Einheiten wie möglich verteilt wird.	Richtlinien zur Konfiguration von Speicherpools finden Sie in "Planung für Speicherpools auf DISK- oder FILE-Einheiten". Informationen zum Definieren der Variable *DB2_PARALLEL_IO* finden Sie in Empfohlene Einstellungen für IBM Db2-Registry-Variablen.
Haben Sie tägliche Operationen auf der Basis Ihrer Sicherungsstrategie geplant?	Die Operationsfolge sieht gemäß den bewährten Verfahren wie folgt aus: 1. Clientsicherung 2. Speicherpoolschutz 3. Knotenreplikation 4. Datenbanksicherung 5. Bestandsverfall	• Datendeduplizierungs- und Knotenreplikationsprozesse planen • Tägliche Operation für Verzeichniscontainerspeicherpools
Haben Sie Prüfoperationen geplant, um beschädigte Dateien in Speicherpools zu identifizieren?	Um Prüfoperationen zu planen, verwenden Sie den Befehl **DEFINE STGRULE** und geben Sie den Parameter **ACTIONTYPE=AUDIT** an. Um sicherzustellen, dass Prüfoperationen fortlaufend ausgeführt werden, geben Sie als bewährtes Verfahren nicht den Parameter **DELAY** an.	

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Ist genügend Speicher zur Verwaltung der IBM Db2-Sperrenliste vorhanden?	Wenn Sie Daten deduplizieren, die große Dateien oder gleichzeitig eine große Anzahl Dateien umfassen, kann der Prozess zur Speicherknappheit führen. Wenn der Sperrenlistenspeicher nicht ausreichend ist, können Sicherungsfehler, Datenverwaltungsprozessfehler oder Serverausfälle auftreten. Bei Dateigrößen über 500 GB, die durch die Datendeduplizierung verarbeitet werden, ist es sehr wahrscheinlich, dass der Speicherplatz knapp wird. Wenn jedoch viele Sicherungsoperationen die clientseitige Datendeduplizierung verwenden, kann dieses Problem auch bei Dateien mit geringerer Größe auftreten.	Informationen zur Optimierung des Db2-Parameters **LOCKLIST** finden Sie in Serverseitige Datendeduplizierung optimieren.
Ist genügend Bandbreite verfügbar, um Daten auf einen IBM Spectrum Protect-Server zu übertragen?	Um Daten auf einen IBM Spectrum Protect-Server zu übertragen, verwenden Sie die clientseitige oder serverseitige Datendeduplizierung und die Komprimierung, um die erforderliche Bandbreite zu verringern. Verwenden Sie einen Server der Version 7.1.5 oder höher, um die Inline-Komprimierung verwenden zu können, und einen Client der Version 7.1.6 oder höher, um die erweiterte Komprimierungsverarbeitung zu aktivieren.	Weitere Informationen finden Sie in der Beschreibung der Clientoption **enablededup**.
Haben Sie festgelegt, wie viele Speicherpoolverzeichnisse jedem Speicherpool zugeordnet werden sollen?	Ordnen Sie Verzeichnisse einem Speicherpool mithilfe des Befehls **DEFINE STGPOOLDIRECTORY** zu. Erstellen Sie mehrere Speicherpoolverzeichnisse und stellen Sie sicher, dass jedes Verzeichnis auf einem anderen Plattendatenträger (LUN) gesichert wird.	

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie genügend Plattenspeicherplatz in dem Cloud-Containerspeicherpool zugeordnet?	Um Sicherungsfehler zu verhindern, stellen Sie sicher, dass das lokale Verzeichnis über genügend Speicherplatz verfügt. Verwenden Sie die folgende Liste als Leitfaden für optimalen Plattenspeicherplatz: • Berechnen Sie für SAS-Platten (SAS = Serial-Attached SCSI) und rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu. • Stellen Sie 3 TB für flash-basierte Speichersysteme mit schnellen Netzverbindungen zu leistungsfähigen On-Premises-Cloudsystemen bereit. • Stellen Sie 5 TB für Systeme mit Solid-State-Laufwerk (SSD) mit schnellen Netzverbindungen zu leistungsfähigen Cloudsystemen bereit.	

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie den geeigneten Typ des lokalen Speichers ausgewählt?	Stellen Sie sicher, dass Datenübertragungen aus dem lokalen Speicher in die Cloud beendet werden, bevor der nächste Sicherungszyklus beginnt. **Tipp:** Daten werden kurz nach dem Versetzen in die Cloud aus dem lokalen Speicher entfernt. Verwenden Sie die folgenden Richtlinien: • Verwenden Sie Flash- oder SSD-Speicher für große Systeme, die über leistungsfähige Cloudsysteme verfügen. Stellen Sie sicher, dass Sie über eine dedizierte 10-GB-WAN-Verbindung mit einer Hochgeschwindigkeitsverbindung zum Objektspeicher verfügen. Verwenden Sie beispielsweise Flash- oder SSD-Speicher, wenn Sie über eine dedizierte 10-GB-WAN-Verbindung sowie eine Hochgeschwindigkeitsverbindung zu einem IBM Cloud Object Storage-Speicherort oder zu einem Amazon S3-Datencenter (Amazon S3 = Amazon Simple Storage Service) verfügen. • Verwenden Sie SAS-Platten mit 15000 U/min mit größerer Kapazität für die folgenden Szenarios: – Systeme mittlerer Größe – Langsamere Cloudverbindungen, z. B. 1 GB – Bei Verwendung von IBM Cloud Object Storage als Service-Provider in mehreren Regionen • Berechnen Sie für SAS-Platten oder rotierende Platten das Volumen neuer Daten, das nach der täglichen Datenreduktion (Komprimierung und Datendeduplizierung) erwartet wird. Ordnen Sie bis zu 100 Prozent dieses Volumens (in Terabyte) für den Plattenspeicherplatz zu.	

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie für Cloud-Containerspeicherpools die maximale Gesamtzahl paralleler Prozesse für die Speicherregel und alle untergeordneten Regeln angegeben?	Um die maximale Anzahl paralleler Prozesse anzugeben, geben Sie den Befehl **DEFINE STGRULE** aus und geben Sie den Parameter **MAXPROCESS** an. Der Standardwert ist 8. Wenn beispielsweise der Standardwert 8 angegeben wird und die Speicherregel vier untergeordnete Regeln hat, kann die Speicherregel acht parallele Prozesse ausführen und jede untergeordnete Regel kann acht parallele Prozesse ausführen. Verwenden Sie für einen optimalen Durchsatz die folgende maximale Anzahl paralleler Prozesse für kleine, mittelgroße und große Blueprint-Systeme: • Kleines System: 10 Prozesse • Mittelgroßes System: 25 Prozesse • Großes System: 35-50 Prozesse	
Haben Sie für Cloud-Containerspeicherpools mehrere Accesser-Endpunkte definiert, wenn ein lokales IBM Cloud Object Storage-System mit IBM Spectrum Protect verwendet wird?	Um die Leistung zu optimieren, definieren Sie abhängig von den Anforderungen an die Datenaufnahme exklusiven Zugriff für die folgende Anzahl Accesser für kleine, mittelgroße und große Blueprint-Systeme: • Kleines System: 1 Accesser • Mittelgroßes System: 2 Accesser • Großes System: 3-4 Accesser	Weitere Informationen finden Sie in den IBM Spectrum Protect Cloud Blueprints.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie für Cloud-Containerspeicherpools mehrere Accesser-Endpunkte definiert, wenn ein lokales IBM Cloud Object Storage-System mit IBM Spectrum Protect verwendet wird?	Im Allgemeinen ist die folgende Ethernet-Funktionalität erforderlich, um eine Verbindung zu privaten IBM Cloud Object Storage-Endpunkten für kleine, mittelgroße und große Blueprint-Systeme herzustellen: • Kleines System: 1 Gigabit • Mittelgroßes System: 5 Gigabit • Großes System: 10 Gigabit **Tipp:** Abhängig von der Clientdatenaufnahme und der simultanen Übertragung von Daten in den Objektspeicher sind möglicherweise mehrere 10-Gigabit-Ethernet-Netze erforderlich. Wenn Sie die Ethernet-Verbindung konfigurieren, arbeiten Sie mit einem Netzadministrator zusammen und ziehen Sie die folgenden Faktoren in Betracht: • Die Ethernet-Funktionalität des Servers • Die Art des Netzes zwischen dem Server und dem IBM Cloud Object Storage-Endpunkt • Der letzte Aufnahmepunkt für den Objektspeicher über einen Cloud-Containerspeicherpool	

Planung für Speicherpools auf DISK- oder FILE-Einheiten

Überprüfen Sie mithilfe der Prüfliste, wie Ihre Plattenspeicherpools konfiguriert sind. Diese Prüfliste umfasst Tipps für Speicherpools, die die Einheitenklasse DISK oder FILE verwenden.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Können die Speicherpool-LUNs Durchsatzraten von 256 KB für sequenzielle Lese- und Schreibvorgänge aufrechterhalten, um die Arbeitslast innerhalb der Zeitvorgaben adäquat handhaben zu können?	Bei der Planung für Spitzenbelastungen müssen Sie alle Daten berücksichtigen, die der Server gleichzeitig aus Plattenspeicherpools lesen oder in Plattenspeicherpools schreiben soll. Berücksichtigen Sie beispielsweise den Spitzenwert für den Datenfluss bei Clientsicherungsoperationen und Serverdatenversetzungsoperationen, wie z. B. Umlagerung, die gleichzeitig ausgeführt werden. Der IBM Spectrum Protect-Server verwendet beim Lesen aus Speicherpools und Schreiben in Speicherpools in erster Linie 256-KB-Blöcke. Wenn das Plattensystem über die entsprechende Funktionalität verfügt, konfigurieren Sie das Plattensystem für die optimale Leistung mit sequenziellen Lese-/Schreiboperationen statt mit wahlfreien Lese-/Schreiboperationen.	Weitere Informationen finden Sie in Basisleistung von Plattensystemen analysieren.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie genügend Speicherplatz für die Datenbank zugeordnet?	Als grobe Schätzung basieren die folgenden Richtlinien für die Datenbankgröße auf den kleinen, mittelgroßen und großen Blueprint-Systemen, um Datenbankwachstum zu ermöglichen: • Kleines System: Mindestens 1 TB • Mittelgroßes System: Mindestens 2 TB • Großes System: Mindestens 4 TB **Tipp:** Möglicherweise wird auf der Basis des Datenvolumens, das geschützt werden muss, der Anzahl Dateien, die gespeichert werden, und der Verwendung der Datendeduplizierung weiterer Speicher benötigt. Bei der Datendeduplizierung wird die Last auf die Datenbank größer, da die Datenbank häufig abgefragt wird, um festzustellen, welche deduplizierten Speicherbereiche auf dem Server vorhanden sind. Als grobe Schätzung sollten Sie 100 GB Datenbankspeicher für jeweils 50 TB Daten einplanen, die in deduplizierten Speicherpools geschützt werden sollen. Geschützte Daten ist das Datenvolumen vor der Datendeduplizierung, einschließlich aller Versionen gespeicherter Objekte. Wenn Sie mehrere Hundert TB geschützter Daten haben oder wenn Sie täglich mehrere TB Daten sichern, muss die Anfangsgröße der Datenbank mindestens 1 TB sein. Verwenden Sie IBM Spectrum Protect, um die Größe der Datenbank für Ihr System festzulegen.	Die optimale IBM Spectrum Protect-Umgebung wird mithilfe der IBM Spectrum Protect-Blueprints konfiguriert. Informationen zur minimalen Speicherkapazität, die auf der Basis der Datenbankgröße auf dem Server zugeordnet werden muss, um Operationen auszuführen, finden Sie in Speicherbedarf.
Ist die Platte für die Verwendung von Lese- und Schreibcache konfiguriert?	Verwenden Sie mehr Cache, um eine bessere Leistung zu erzielen.	

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Müssen Sie die IBM Spectrum Protect-Datenbank im Cloudobjektspeicher sichern?	Zu Zwecken der Wiederherstellung nach einem Katastrophenfall können Sie eine Datenbank im Cloudobjektspeicher sichern und aus dem Cloudobjektspeicher zurückschreiben. Sie können Objektspeicherendpunkte, IBM Cloud Object Storage-Accesser, Netzbandbreite und Datenströme optimieren, um sicherzustellen, dass Datenbanksicherungsoperationen effizient ausgeführt werden.	Datenbanksicherungen in Cloudobjektspeicher optimieren.
Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, eine geeignete Größe für die Speicherpooldatenträger festgelegt?	Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden. Wenn Sie nicht über die nötigen Informationen zum Schätzen der Größe für Datenträger mit der Einheitenklasse FILE verfügen, beginnen Sie mit einer Datenträgergröße von 50 GB.	In der Regel treten häufiger Probleme auf, wenn die Datenträger zu klein sind. Wenn Datenträger größer als erforderlich sind, treten nur selten Probleme auf. Wenn Sie die zu verwendende Datenträgergröße festlegen, sollten Sie als Vorsichtsmaßnahme eine größere Größe als erforderlich wählen.
Verwenden Sie für Speicherpools, die die Einheitenklasse FILE verwenden, vorab zugeordnete Datenträger?	Arbeitsdatenträger können eine Dateifragmentierung zur Folge haben. Um sicherzustellen, dass für einen Speicherpool immer genügend Datenträger verfügbar sind, setzen Sie den Parameter **MAXSCRATCH** auf einen Wert größer als null.	Ordnen Sie mithilfe des Befehls **DEFINE VOLUME** Datenträger in dem Speicherpool vorab zu. Verwenden Sie den Serverbefehl **DEFINE STGPOOL** oder **UPDATE STGPOOL**, um den Parameter **MAXSCRATCH** zu definieren.
Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, die maximale Anzahl Clientsitzungen mit der Anzahl definierter Datenträger verglichen?	Es müssen immer genügend verwendbare Datenträger in den Speicherpools vorhanden sein, um die erwartete maximale Anzahl gleichzeitig ausgeführter Clientsitzungen handhaben zu können. Bei den Datenträgern kann es sich um Arbeitsdatenträger, leere Datenträger oder teilweise gefüllte Datenträger handeln.	Bei Speicherpools, die die Einheitenklasse FILE verwenden, kann jeweils nur eine einzige Sitzung oder ein einziger Prozess auf einen Datenträger schreiben.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie für Speicherpools, die die Einheitenklasse FILE verwenden, den Parameter **MOUNTLIMIT** für die Einheitenklasse auf einen Wert gesetzt, der für die Anzahl Datenträger, die parallel angehängt werden könnten, ausreichend hoch ist?	Für Speicherpools, die die Datendeduplizierung verwenden, liegt der Wert für den Parameter **MOUNTLIMIT** in der Regel zwischen 500 und 1000. Setzen Sie den Wert für **MOUNTLIMIT** auf die maximale Anzahl Mountpunkte, die für alle aktiven Sitzungen erforderlich sind. Berücksichtigen Sie Parameter, die sich auf die maximale Anzahl erforderlicher Mountpunkte auswirken: • Die Serveroption **MAXSESSIONS**, die die maximal zulässige Anzahl gleichzeitig ablaufender IBM Spectrum Protect-Sitzungen angibt • Der Parameter **MAXNUMMP**, der die maximale Anzahl Mountpunkte definiert, die jeder Clientknoten verwenden kann Wenn beispielsweise die maximalen Anzahl Sicherungssitzungen für Clientknoten normalerweise 100 ist und für jeden der Knoten MAXNUMMP=2 definiert ist, multiplizieren Sie 100 Knoten mit 2 Mountpunkten für jeden Knoten, um den Wert 200 für den Parameter **MOUNTLIMIT** zu erhalten.	Verwenden Sie den Serverbefehl **REGISTER NODE** oder **UPDATE NODE**, um den Parameter **MAXNUMMP** für Clientknoten zu definieren.

Frage	Tasks, Merkmale, Optionen oder Einstellungen	Weitere Informationen
Haben Sie für Speicherpools, die die Einheitenklasse DISK verwenden, festgelegt, wie viele Speicherpooldatenträger in jedes Dateisystem gestellt werden sollen?	Die Konfiguration des Speichers für einen Speicherpool, der eine Einheitenklasse DISK verwendet, ist davon abhängig, ob Sie RAID für das Plattensystem verwenden. Wenn Sie RAID nicht verwenden, konfigurieren Sie ein einzige Dateisystem pro physischer Platte und definieren Sie exakt einen Speicherpooldatenträger für jedes Dateisystem. Wenn Sie RAID 5 mit *n* + 1 Datenträgern verwenden, konfigurieren Sie den Speicher auf eine der folgenden Arten: • Konfigurieren Sie *n* Dateisysteme auf der LUN und definieren Sie exakt einen Speicherpooldatenträger pro Dateisystem. • Konfigurieren Sie ein einziges Dateisystem und *n* Speicherpooldatenträger für die LUN.	Ein Beispiellayout, bei dem diese Richtlinie eingehalten wird, zeigt Beispiellayout für Serverspeicherpools.
Haben Sie Ihre Speicherpools für die Verteilung der Ein-/Ausgabe auf mehrere Dateisysteme erstellt?	Stellen Sie sicher, dass sich jedes Dateisystem auf einer anderen LUN auf dem Plattensystem befindet. Normalerweise sind 10-30 Dateisysteme ein geeigneter Wert, Sie müssen jedoch sicherstellen, dass die Dateisysteme nicht kleiner als etwa 250 GB sind.	Ausführliche Informationen finden Sie in: • Plattenspeicher für den Server optimieren • Speicherpools und Datenträger optimieren und konfigurieren
Haben Sie Prüfoperationen geplant, um beschädigte Dateien in Speicherpools zu identifizieren?	Um Prüfoperationen zu planen, verwenden Sie den Befehl **DEFINE STGRULE** und geben Sie den Parameter **ACTIONTYPE=AUDIT** an. Um Prüfoperationen zu optimieren und sicherzustellen, dass sie fortlaufend ausgeführt werden, geben Sie nicht den Parameter **DELAY** an.	

Planung für die Auswahl des korrekten Speichertechnologietyps

Speichereinheiten haben eine unterschiedliche Kapazität und unterschiedliche Leistungsmerkmale. Diese Merkmale wirken sich darauf aus, welche Einheiten besser für die Verwendung mit IBM Spectrum Protect geeignet sind.

Prozedur

- Die folgende Tabelle unterstützt Sie bei der Auswahl des korrekten Speichertechnologietyps für die Speicherressourcen, die der Server erfordert.

Tabelle 5. Speichertechnologietypen für IBM Spectrum Protect-Speicherbedarf

Speichertechnologietyp	Datenbank	Aktive Protokolldatei	Archivprotokoll und Archivübernahmeprotokoll	Speicherpools
Solid-State-Laufwerk (SSD)	Stellen Sie die Datenbank auf ein Solid-State-Laufwerk, wenn die folgenden Bedingungen erfüllt sind: – Sie verwenden die IBM Spectrum Protect-Datendeduplizierung. – Sie sichern täglich mehr als 8 TB neuer Daten.	Wenn Sie die IBM Spectrum Protect-Datenbank auf ein Solid-State-Laufwerk stellen (dies ist das bewährte Verfahren), stellen Sie auch die aktive Protokolldatei auf ein Solid-State-Laufwerk. Wenn kein Speicherplatz verfügbar ist, verwenden Sie stattdessen eine Hochleistungsplatte.	Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Das Archivprotokoll und die Archivübernahmeprotokolle können auf langsamere Speichertechnologietypen gestellt werden.	Reservieren Sie die Solid-State-Laufwerke für die Verwendung mit der Datenbank und der aktiven Protokolldatei. Speicherpools können auf langsamere Speichertechnologietypen gestellt werden.
Hochleistungsplatte mit den folgenden Kenndaten: **– Platte mit 15.000 U/min** **– Fibre Channel- oder Serial-attached SCSI-Schnittstelle (SAS-Schnittstelle)**	Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind: – Der Server führt keine Datendeduplizierung aus. – Der Server führt keine Knotenreplikation aus. Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.	Verwenden Sie Hochleistungsplatten, wenn die folgenden Bedingungen erfüllt sind: – Der Server führt keine Datendeduplizierung aus. – Der Server führt keine Knotenreplikation aus. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.	Sie können Hochleistungsplatten für das Archivprotokoll und die Archivübernahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.	Verwenden Sie Hochleistungsplatten für Speicherpools, wenn die folgenden Bedingungen erfüllt sind: – Daten werden häufig gelesen. – Daten werden häufig geschrieben. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.

Tabelle 5. Speichertechnologietypen für IBM Spectrum Protect-Speicherbedarf (Forts.)

Speichertechnologietyp	Datenbank	Aktive Protokolldatei	Archivprotokoll und Archivübernahmeprotokoll	Speicherpools
Platte mit mittlerer Leistung oder Hochleistungsplatte mit den folgenden Kenndaten: **– Platte mit 10.000 U/min** **– Fibre Channel- oder SAS-Schnittstelle**	Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie die Serverdatenbank von den zugehörigen Protokollen und Speicherpools sowie von Daten für andere Anwendungen.	Wenn das Plattensystem eine Kombination verschiedener Plattentechnologien verwendet, verwenden Sie die schnelleren Platten für die Datenbank und die aktive Protokolldatei. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die aktive Protokolldatei von der Serverdatenbank, den Archivprotokollen und den Speicherpools.	Sie können eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für das Archivprotokoll und die Archivübernahmeprotokolle verwenden. Trennen Sie aus Gründen der Verfügbarkeit diese Protokolle von der Datenbank und der aktiven Protokolldatei.	Verwenden Sie eine Platte mit mittlerer Leistung oder eine Hochleistungsplatte für Speicherpools, wenn die folgenden Bedingungen erfüllt sind: – Daten werden häufig gelesen. – Daten werden häufig geschrieben. Trennen Sie aus Gründen der Leistung und Verfügbarkeit die Speicherpooldaten von der Serverdatenbank und den Protokollen sowie von Daten für andere Anwendungen.
SATA, Network-attached Storage (NAS)	Verwenden Sie diesen Speicher nicht für die Datenbank. Stellen Sie die Datenbank nicht auf XIV-Speichersysteme.	Verwenden Sie diesen Speicher nicht für die aktive Protokolldatei.	Die Verwendung dieser langsameren Speichertechnologie ist akzeptabel, da diese Protokolle einmal geschrieben und nur selten gelesen werden.	Verwenden Sie diese langsamere Speichertechnologie, wenn die folgenden Bedingungen erfüllt sind: – Daten werden selten geschrieben, beispielsweise einmal. – Daten werden selten gelesen. .
Bänder und virtuelle Bänder				Verwenden Sie diese Speichermedien für die langfristige Aufbewahrung oder wenn Daten nur selten verwendet werden.

Bewährte Verfahren bei der Serverinstallation anwenden

Normalerweise hat die Konfiguration und Auswahl der Hardware die deutlichsten Auswirkungen auf die Leistung einer IBM Spectrum Protect-Lösung. Weitere Faktoren, die sich auf die Leistung auswirken, sind die Auswahl und Konfiguration des Betriebssystems sowie die Konfiguration von IBM Spectrum Protect.

Prozedur

- Nachfolgend sind die wichtigsten bewährten Verfahren für die Erzielung der optimalen Leistung und die Vermeidung von Problemen aufgeführt.
- Bestimmen Sie anhand der Tabelle die bewährten Verfahren, die für Ihre Umgebung gelten.

Bewährtes Verfahren	Weitere Informationen
Verwenden Sie schnelle Platten für die Serverdatenbank. Enterprise-Solid-State-Laufwerke mit Fibre Channel- oder SAS-Schnittstellen bieten die beste Leistung.	Verwenden Sie schnelle Platten mit kurzer Latenzzeit für die Datenbank. Die Verwendung von Solid-State-Laufwerken ist von entscheidender Bedeutung, wenn Sie die Datendeduplizierung und Knotenreplikation verwenden. Vermeiden Sie die Verwendung von SATA-Laufwerken (SATA = Serial Advanced Technology Attachment) und PATA-Laufwerken (PATA = Parallel Advanced Technology Attachment). Ausführliche Informationen und weitere Tipps finden Sie in: – "Planung für Platten für die Serverdatenbank" – "Planung für die Auswahl des korrekten Speichertechnologietyps"
Stellen Sie sicher, dass das Serversystem über genügend Speicher verfügt.	Überprüfen Sie die Betriebssystemvoraussetzungen in Technote 84861. Höhere Arbeitslasten erfordern mehr als die Mindestvoraussetzungen. Erweiterte Funktionen wie beispielsweise Datendeduplizierung und Knotenreplikation können mehr Speicher als den Mindestspeicher erfordern, der im Dokument mit den Systemvoraussetzungen angegeben ist. Wenn Sie die Ausführung mehrerer Instanzen planen, ist für jede Instanz der für einen einzelnen Server aufgelistete Speicher erforderlich. Multiplizieren Sie den für einen einzelnen Server erforderlichen Speicher mit der Anzahl der für das System geplanten Instanzen.
Trennen Sie die Serverdatenbank, die aktive Protokolldatei, das Archivprotokoll und die Plattenspeicherpools voneinander.	Stellen Sie alle IBM Spectrum Protect-Speicherressourcen auf unterschiedliche Platten. Trennen Sie Speicherpoolplatten von den Platten für die Serverdatenbank und die Protokolle. Speicherpooloperationen können Datenbankoperationen beeinträchtigen, wenn sich die Speicherpools und die Datenbank auf denselben Platten befinden. Im Idealfall werden auch die Serverdatenbank und die Protokolle voneinander getrennt. Ausführliche Informationen und weitere Tipps finden Sie in: – "Planung für Platten für die Serverdatenbank" – "Planung für Platten für das Serverwiederherstellungsprotokoll" – "Planung für Speicherpools auf DISK- oder FILE-Einheiten"
Verwenden Sie mindestens vier Verzeichnisse für die Serverdatenbank. Verwenden Sie für größere Server oder Server, die erweiterte Funktionen verwenden, acht Verzeichnisse.	Stellen Sie jedes Verzeichnis auf eine LUN, die von anderen LUNs und von anderen Anwendungen getrennt ist. Ein Server wird als großer Server betrachtet, wenn seine Datenbank größer als 2 TB ist oder wahrscheinlich diese Größe erreichen wird. Verwenden Sie für derartige Server acht Verzeichnisse. Siehe "Planung für Platten für die Serverdatenbank".

Bewährtes Verfahren	Weitere Informationen
Wenn Sie die Datendeduplizierung und/oder die Knotenreplikation verwenden, beachten Sie die Richtlinien für die Datenbankkonfiguration und andere Elemente.	Konfigurieren Sie den Server gemäß den Richtlinien, da die Datenbank in Bezug darauf, wie gut die Ausführung des Servers bei Verwendung dieser Funktionen ist, extrem wichtig ist. Ausführliche Informationen und weitere Tipps finden Sie in: – Prüfliste für Datendeduplizierung – Prüfliste für Knotenreplikation
Beachten Sie bei Speicherpools, die Einheitenklassen des Typs FILE verwenden, die Richtlinien für die Größe von Speicherpooldatenträgern. In der Regel sind Datenträger mit einer Größe von 50 GB am besten geeignet.	Lesen Sie die Informationen in Optimale Anzahl und Größe von Datenträgern für Speicherpools, die Platten verwenden zur Bestimmung der Datenträgergröße. Konfigurieren Sie Speicherpooleinheiten und Dateisysteme auf der Basis der Anforderungen in Bezug auf den Durchsatz und nicht nur auf der Basis der Kapazitätsanforderungen. Trennen Sie die Speichereinheiten, die von IBM Spectrum Protect verwendet werden, von anderen Anwendungen mit hoher Ein-/Ausgabe und stellen Sie sicher, dass der Durchsatz für diesen Speicher ausreichend ist. Weitere ausführliche Informationen finden Sie in Prüfliste für Speicherpools auf FILE- oder DISK-Einheiten.
Planen Sie IBM Spectrum Protect-Clientoperationen und -Serververwaltungsaktivitäten, um eine Überschneidung von Operationen zu verhindern oder auf ein Mindestmaß zu reduzieren.	Weitere ausführliche Informationen liefern die folgenden Themen: – Zeitplan für tägliche Operationen optimieren – Prüfliste für Serverkonfiguration
Überwachen Sie Operationen kontinuierlich.	Die Überwachung ermöglicht es Ihnen, Probleme frühzeitig erkennen und Ursachen leichter ermitteln zu können. Bewahren Sie Aufzeichnungen von Überwachungsberichten bis zu einem Jahr lang auf, um Trends schneller erkennen und Wachstum besser planen zu können. Siehe Umgebung im Hinblick auf die Leistung überwachen und verwalten.

Systemmindestvoraussetzungen

Für die Installation des IBM Spectrum Protect-Servers auf einem Linux-System wird ein Minimum an Hardware und Software benötigt. Hierzu gehören eine Übertragungsmethode (Kommunikationsverfahren) und der aktuelle Einheitentreiber.

Die optimale IBM Spectrum Protect-Umgebung ist mit Datendeduplizierung mithilfe der IBM Spectrum Protect Blueprints konfiguriert.

Das IBM Spectrum Protect-Einheitentreiberpaket enthält keinen Einheitentreiber für dieses Betriebssystem, weil ein generischer SCSI-Einheitentreiber verwendet wird. Konfigurieren Sie den Einheitentreiber, bevor der IBM Spectrum Protect-Server für Bandeinheiten verwendet wird. Das IBM Spectrum Protect-Treiberpaket enthält Treibertools und ACSLS-Dämonen. IBM-Treiberpakete finden Sie auf der Fix Central-Website.

Informationen zu Voraussetzungen, unterstützten Einheiten, Clientinstallationspaketen und Fixes sind im IBM Support Portal for IBM Spectrum Protect verfügbar. Rufen Sie nach der Installation von IBM Spectrum Protect und vor der individuellen Anpassung die Website auf, laden Sie alle anwendbaren Fixes herunter und wenden Sie diese Fixes an.

Servermindestvoraussetzungen für Linux x86_64

Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux x86_64-Betriebssystem installieren.

Hardware- und Softwarevoraussetzungen für die IBM Spectrum Protect-Serverinstallation

Die neuesten Informationen zu den IBM Spectrum Protect-Systemvoraussetzungen finden Sie in Technote 84861.

In Tabelle 1 sind die für einen Server auf einem Linux x86_64-System erforderlichen Hardwaremindestvoraussetzungen beschrieben.

Tabelle 6. Hardwarevoraussetzungen

Hardwaretyp	Hardwarevoraussetzungen
Allgemein	Ein AMD64- oder Intel EM64T-Prozessor
Plattenspeicher	Folgende Mindestwerte für den Plattenspeicher: • 4,3 GB für das Installationsverzeichnis • 2,5 GB für das Verzeichnis `/var` • 4 GB für das Verzeichnis `/tmp` • 128 MB im Ausgangsverzeichnis des Rootbenutzers • 2 GB für den Bereich der gemeinsam genutzten Ressourcen Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben. Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten. Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN. Lesen Sie den Abschnitt zur „Kapazitätsplanung” auf Seite 61, um weitere Informationen zum Plattenspeicherplatz zu erhalten.

Tabelle 6. Hardwarevoraussetzungen (Forts.)	
Hardwaretyp	**Hardwarevoraussetzungen**
Hauptspeicher	Folgende Mindestwerte für den Hauptspeicher: • 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation • 24 GB für Datendeduplizierung oder Knotenreplikation • 32 GB für Knotenreplikation mit Datendeduplizierung Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect. Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.

Softwarevoraussetzungen

In Tabelle 2 sind die für einen Server auf einem Linux x86_64-System erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 7. Softwarevoraussetzungen	
Softwaretyp	**Softwaremindestvoraussetzungen**
Betriebssystem	Für den IBM Spectrum Protect-Server unter Linux x86_64 ist eines der folgenden Betriebssysteme erforderlich: • Red Hat Enterprise Linux 8.1 oder höher • Red Hat Enterprise Linux 7.6 oder höher • SUSE Linux Enterprise Server 15, SP1 oder höher • SUSE Linux Enterprise Server 12, SP4 oder höher • Ubuntu Server LTS, Version 16.04.2 oder 18.04. Die minimale Versionsnummer für Bandspeicher ist Ubuntu Server LTS Version 18.04.

Tabelle 7. Softwarevoraussetzungen (Forts.)

Softwaretyp	Softwaremindestvoraussetzungen
Bibliotheken	Auf dem IBM Spectrum Protect-System installierte GNU C-Bibliotheken Version 2.3.3-98.38 oder höher. Für Red Hat Enterprise Linux Server: • libaio • libstdc++.so.6 (32- und 64-Bit-Pakete sind erforderlich) • numactl.x86_64 Fügen Sie für Red Hat Enterprise Linux (RHEL 8) außerdem die folgende Bibliothek hinzu: • libnsl.so.1 • libnuma.so.1 Für SUSE Linux Enterprise Server: • libaio • libstdc++.so.6 Version 4.3 oder höher (32- und 64-Bit-Pakete sind erforderlich) • libnuma.so.1 Für Ubuntu LTS Server: • libaio1 • libnuma.so.1 Führen Sie einen der folgenden Schritte aus, um festzustellen, ob SELinux installiert ist und sich im restriktiven Modus befindet: • Überprüfen Sie die Datei `/etc/sysconfig/selinux`. • Führen Sie den Betriebssystembefehl **`sestatus`** aus. • Überprüfen Sie die Datei `/var/log/messages` auf SELinux-Nachrichten. **Einschränkung:** SELinux muss für IBM Spectrum Protect-Installationen und -Upgrades inaktiviert werden. Führen Sie einen der folgenden Schritte aus, um SELinux zu inaktivieren: • Geben Sie den toleranten Modus an, indem Sie den Befehl `setenforce 0` als Superuser ausgeben. • Ändern Sie die Datei `/etc/sysconfig/selinux` und führen Sie einen Neustart der Maschine durch.
Übertragungsprotokoll	• TCP/IP Version 4 oder Version 6 (Standard für Linux) • Shared Memory-Protokoll (mit IBM Spectrum Protect Linux x86_64-Client)
Verarbeitung	Asynchrone Ein-/Ausgabe muss aktiviert sein. Installieren Sie für Linux-Kernel mit 2.6 oder höher die Bibliothek libaio, um die asynchrone Ein-/Ausgabe zu aktivieren.

Tabelle 7. Softwarevoraussetzungen (Forts.)	
Softwaretyp	**Softwaremindestvoraussetzungen**
Einheitentreiber	Der IBM Spectrum Protect-Durchgriffseinheitentreiber wird für Einheiten eines anderen Herstellers verwendet. Er verwendet die SCSI-Durchgriffsschnittstelle für die Kommunikation mit Bandeinheiten und Bandarchiven. Der generische Linux-SCSI-Einheitentreiber (sg) ist für Bandlaufwerke und Bandarchive erforderlich. Das IBM Spectrum Protect-Einheitentreiberpaket enthält Einheitentreibertools und ACSLS-Dämonen. Für die Bandarchive bzw. Bandlaufwerke IBM 3590, 3592 oder Ultrium sind die IBM Einheitentreiber erforderlich. Installieren Sie die aktuellen Einheitentreiber. IBM Treiberpakete finden Sie in Fix Central. Konfigurieren Sie die Einheitentreiber, bevor Sie den IBM Spectrum Protect-Server für Bandeinheiten verwenden.
Sonstige Software	• Korn-Shell (ksh) • Damit IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) authentifiziert werden können, müssen Sie einen der folgenden Verzeichnisserver verwenden: – Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2, Windows Server 2016) – IBM Security Directory Server Version 6.3 – IBM Security Directory Server Version 6.4

Servermindestvoraussetzungen für Linux on System z

Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux on System z-Betriebssystem installieren.

Hardware- und Softwarevoraussetzungen für die IBM Spectrum Protect-Serverinstallation

Die neuesten Informationen zu den IBM Spectrum Protect-Systemvoraussetzungen finden Sie in Technote 1243309.

In Tabelle 1 sind die für Ihr IBM Spectrum Protect-System unter Linux on System z erforderlichen Hardwaremindestvoraussetzungen beschrieben. Weitere Informationen zur Planung des Plattenspeicherplatzes finden Sie in „Kapazitätsplanung” auf Seite 61.

Tabelle 8. Hardwarevoraussetzungen	
Hardwaretyp	**Hardwarevoraussetzungen**
Allgemein	Native logische Partition (LPAR) für IBM zSeries, IBM System z9, IBM System z10 oder IBM zEnterprise System (z114 und z196) 64-Bit oder z/VM-Gast.

Tabelle 8. Hardwarevoraussetzungen (Forts.)

Hardwaretyp	Hardwarevoraussetzungen
Plattenspeicher	Folgende Mindestwerte für den Plattenspeicher: • 4,3 GB für das Installationsverzeichnis • 2,5 GB für das Verzeichnis `/var` • 4 GB für das Verzeichnis `/tmp` • 128 MB im Ausgangsverzeichnis des Rootbenutzers • 2 GB für den Bereich der gemeinsam genutzten Ressourcen Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben. Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten. Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN. Lesen Sie den Abschnitt zur „Kapazitätsplanung” auf Seite 61, um weitere Informationen zum Plattenspeicherplatz zu erhalten.
Hauptspeicher	Folgende Mindestwerte für den Hauptspeicher: • 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation • 24 GB für Datendeduplizierung oder Knotenreplikation • 32 GB für Knotenreplikation mit Datendeduplizierung Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect. Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.

Softwarevoraussetzungen

In Tabelle 2 sind die für Ihr IBM Spectrum Protect-System unter Linux on System z erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 9. Softwarevoraussetzungen

Softwaretyp	**Softwaremindestvoraussetzungen**
Betriebssystem	Für den IBM Spectrum Protect-Server unter Linux on System z (s390x 64-Bit-Architektur) ist eines der folgenden Betriebssysteme erforderlich: • Red Hat Enterprise Linux 7.6 oder höher • SUSE Linux Enterprise Server 12, SP4 oder höher **Einschränkung:** Die SAN-Erkennungsfunktion wird nicht unterstützt.
Bibliotheken	Auf dem IBM Spectrum Protect-System installierte GNU C-Bibliotheken Version 2.3.3-98.38 oder höher. Für Red Hat Enterprise Linux Server: • libaio • libstdc++.so.6 (32- und 64-Bit-Pakete sind erforderlich) • libxlc-1.2.0.0.151119a.s390x oder höher Für SUSE Linux Enterprise Server: • libaio • libstdc++.so.6 Version 4.3 oder höher (32- und 64-Bit-Pakete sind erforderlich) • libxlc-1.2.0.0.151119a.s390x oder höher Führen Sie einen der folgenden Schritte aus, um festzustellen, ob SELinux installiert ist und sich im restriktiven Modus befindet: • Überprüfen Sie die Datei `/etc/sysconfig/selinux`. • Führen Sie den Betriebssystembefehl **`sestatus`** aus. • Überprüfen Sie die Datei `/var/log/messages` auf SELinux-Nachrichten. **Einschränkung:** SELinux muss für IBM Spectrum Protect-Installationen und -Upgrades inaktiviert werden. Führen Sie einen der folgenden Schritte aus, um SELinux zu inaktivieren: • Geben Sie den toleranten Modus an, indem Sie den Befehl `setenforce 0` als Superuser ausgeben. • Ändern Sie die Datei `/etc/sysconfig/selinux` und führen Sie einen Neustart der Maschine durch.
Übertragungsprotokoll	• TCP/IP Version 4 oder Version 6 (Standard für Linux) • Shared Memory-Protokoll (mit IBM Spectrum Protect Linux s390x-Client)
Verarbeitung	Asynchrone Ein-/Ausgabe muss aktiviert sein. Installieren Sie für Linux-Kernel mit 2.6 oder höher die Bibliothek libaio, um die asynchrone Ein-/Ausgabe zu aktivieren.

Tabelle 9. Softwarevoraussetzungen (Forts.)

Softwaretyp	Softwaremindestvoraussetzungen
Einheitentreiber	Der IBM Spectrum Protect-Durchgriffseinheitentreiber wird für Einheiten eines anderen Herstellers verwendet. Er verwendet die SCSI-Durchgriffsschnittstelle für die Kommunikation mit Bandeinheiten und Bandarchiven. Der generische Linux-SCSI-Einheitentreiber (sg) ist für Bandlaufwerke und Bandarchive erforderlich. Das IBM Spectrum Protect-Einheitentreiberpaket enthält Einheitentreibertools und ACSLS-Dämonen. Für die Bandarchive bzw. Bandlaufwerke IBM 3590, 3592 oder Ultrium sind die IBM Einheitentreiber erforderlich. Installieren Sie die aktuellen Einheitentreiber. IBM Treiberpakete finden Sie in Fix Central. Konfigurieren Sie die Einheitentreiber, bevor Sie den IBM Spectrum Protect-Server für Bandeinheiten verwenden.
Sonstige Software	• Korn-Shell (ksh) • Damit IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) authentifiziert werden können, müssen Sie einen der folgenden Verzeichnisserver verwenden: – Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2, Windows Server 2016) – IBM Security Directory Server Version 6.3 – IBM Security Directory Server Version 6.4

Servermindestvoraussetzungen für Linux on Power Systems (Little Endian)

Überprüfen Sie die Hardware- und Softwarevoraussetzungen, bevor Sie einen IBM Spectrum Protect-Server in einem Linux on Power Systems-Betriebssystem (Little Endian) installieren.

Hardware- und Softwarevoraussetzungen für die IBM Spectrum Protect-Serverinstallation

Die neuesten Informationen zu den IBM Spectrum Protect-Systemvoraussetzungen finden Sie in Technote 1243309.

In Tabelle 10 auf Seite 55 sind die für Ihr System erforderlichen Hardwaremindestvoraussetzungen beschrieben.

Tabelle 10. Hardwarevoraussetzungen

Hardwaretyp	Hardwarevoraussetzungen
Allgemein	Ein Linux on Power Systems-Server (Little Endian) auf einem IBM System. Zum Beispiel ein auf der Website Linux on IBM Power Systems aufgelisteter Server.

Tabelle 10. Hardwarevoraussetzungen (Forts.)

Hardwaretyp	Hardwarevoraussetzungen
Plattenspeicher	Folgender Mindestplattenspeicher: • 4,3 GB für das Installationsverzeichnis • 2,5 GB für das Verzeichnis `/var` • 4 GB für das Verzeichnis `/tmp` • 128 MB im Ausgangsverzeichnis des Rootbenutzers • 2 GB für den Bereich der gemeinsam genutzten Ressourcen Für den Fall, dass ein Problem auftritt und eine Diagnose erforderlich ist, wird empfohlen, temporären oder anderen Speicherbereich für ein FFDC-Protokoll (FFDC = First-Failure Data Capture = Erfassung von Fehlerdaten beim ersten Auftreten) oder für andere temporäre Verwendungszwecke (z. B. für die Erfassung von Traceprotokollen) auf dem System verfügbar zu haben. Sehr viel zusätzlicher Plattenspeicherplatz ist für Datenbank- und Protokolldateien erforderlich. Die Größe der Datenbank ist von der Anzahl der zu speichernden Clientdateien und von der Methode abhängig, mit der sie vom Server verwaltet werden. Der Standardspeicherbereich der aktiven Protokolldatei beträgt 16 GB, das für die meisten Arbeitslasten und Konfigurationen benötigte Minimum. Wenn Sie die aktive Protokolldatei erstellen, benötigen Sie mindestens 64 GB für die Replikation. Wird sowohl Replikation als auch Datendeduplizierung verwendet, erstellen Sie eine aktive Protokolldatei mit einer Größe von 128 GB. Ordnen Sie mindestens die dreifache Größe des Standardspeicherbereichs der aktiven Protokolldatei für das Archivprotokoll zu (48 GB). Stellen Sie sicher, dass Sie über ausreichende Ressourcen verfügen, wenn Sie die Datendeduplizierung verwenden oder eine hohe Clientauslastung erwarten. Für optimale Leistung und zur Erleichterung der Ein-/Ausgabe geben Sie mindestens zwei gleichgroße Container oder Nummern der logischen Einheit (LUN) für die Datenbank an. Darüber hinaus benötigen alle aktiven Protokolldateien und Archivprotokolle einen eigenen Container oder eine eigene LUN. Lesen Sie den Abschnitt zur „Kapazitätsplanung” auf Seite 61, um weitere Informationen zum Plattenspeicherplatz zu erhalten.
Hauptspeicher	• 16 GB für Standardserverbetrieb ohne Datendeduplizierung und Knotenreplikation • 24 GB für Datendeduplizierung oder Knotenreplikation • 32 GB für Knotenreplikation mit Datendeduplizierung Speziellere Angaben zum Speicherbedarf für große Datenbanken und höhere Aufnahmefähigkeit finden Sie in der Tabelle für die Serverspeicheroptimierung von IBM Spectrum Protect. Ausführliche Informationen zum Speicherbedarf bei Verwendung der Datendeduplizierung finden Sie unter IBM Spectrum Protect Blueprint für Ihr Betriebssystem.

Softwarevoraussetzungen

In Tabelle 11 auf Seite 57 sind die für Ihr System erforderlichen Softwaremindestvoraussetzungen beschrieben.

Tabelle 11. Softwarevoraussetzungen

Softwaretyp	Softwaremindestvoraussetzungen
Betriebssystem	Für den IBM Spectrum Protect-Server unter Linux on Power Systems (Little Endian) ist eines der folgenden Betriebssysteme erforderlich: • Red Hat Enterprise Linux 8.1 oder höher • Red Hat Enterprise Linux 7.6 oder höher • SUSE Linux Enterprise Server 15, SP1 oder höher • SUSE Linux Enterprise Server 12, SP4 oder höher **Einschränkung:** Die SAN-Erkennungsfunktion wird nicht unterstützt. • Ubuntu Server LTS, Version 16.04.2 oder 18.04. Die minimale Versionsnummer für Bandspeicher ist Ubuntu Server LTS Version 18.04.
Bibliotheken	GNU-C-Bibliotheken Version 2.4-31.30 und höher. • libaio.so.1 (32- und 64-Bit-Pakete) • libnuma.so.1 Führen Sie einen der folgenden Schritte aus, um festzustellen, ob SELinux installiert ist und sich im restriktiven Modus befindet: • Überprüfen Sie die Datei `/etc/sysconfig/selinux`. • Führen Sie den Betriebssystembefehl **`sestatus`** aus. • Überprüfen Sie die Datei `/var/log/messages` auf SELinux-Nachrichten. **Einschränkung:** SELinux muss für IBM Spectrum Protect-Installationen und -Upgrades inaktiviert werden. Führen Sie einen der folgenden Schritte aus, um SELinux zu inaktivieren: • Führen Sie den Befehl `setenforce 0` als Superuser aus, um den toleranten Modus festzulegen. • Ändern Sie die Datei `/etc/sysconfig/selinux` und führen Sie einen Neustart der Maschine durch.
Übertragungsprotokoll	• TCP/IP Version 4 oder Version 6 (Standard für Linux) • Shared Memory-Protokoll
Verarbeitung	Asynchrone Ein-/Ausgabe muss aktiviert sein. Installieren Sie für Linux-Kernel mit 2.6 oder höher die Bibliothek libaio, um die asynchrone Ein-/Ausgabe zu aktivieren.
Sonstige Software	• Korn-Shell (ksh) • Damit IBM Spectrum Protect-Benutzer mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol) authentifiziert werden können, müssen Sie einen der folgenden Verzeichnisserver verwenden: – Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2, Windows Server 2016) – IBM Security Directory Server Version 6.3 – IBM Security Directory Server Version 6.4

Einschränkung: Unformatierte logische Datenträger werden nicht unterstützt.

Kompatibilität des IBM Spectrum Protect-Servers mit anderen IBM Db2-Produkten auf dem System

Sie können andere Produkte, die Db2-Produkte auf demselben System wie der IBM Spectrum Protect-Server implementieren und verwenden, mit einigen Einschränkungen installieren.

Damit andere Produkte, die ein Db2-Produkt auf demselben System wie der IBM Spectrum Protect-Server verwenden, installiert und verwendet werden können, müssen die folgenden Bedingungen erfüllt sein:

Tabelle 12. Kompatibilität des IBM Spectrum Protect-Servers mit anderen Db2-Produkten auf dem System

Bedingung	**Anweisungen**
Versionsstand	Die anderen Produkte, die ein Db2-Produkt verwenden, müssen Db2 Version 9 oder höher verwenden. Db2-Produkte verfügen ab Version 9 über die Unterstützung für Produktkapselung und -trennung. Ab dieser Version können Sie mehrere Kopien von Db2-Produkten mit unterschiedlichen Codeversionen auf demselben System ausführen. Ausführliche Informationen finden Sie in dem Abschnitt über mehrere Kopien in der Db2-Produktinformation.
Benutzer-IDs und Verzeichnisse	Stellen Sie sicher, dass die Benutzer-IDs, die IDs der abgeschirmten Benutzer, die Installationsposition, andere Verzeichnisse und zugehörige Informationen nicht von mehreren Db2-Installationen gemeinsam genutzt werden. Ihre Angaben müssen sich von den IDs und Positionen unterscheiden, die Sie für die Installation und Konfiguration des IBM Spectrum Protect-Servers verwendet haben. Wenn Sie den Assistenten **dsmicfgx** für die Konfiguration des Servers verwendet haben, haben Sie diese Werte während der Ausführung des Assistenten eingegeben. Wenn Sie eine manuelle Konfiguration durchgeführt haben, überprüfen Sie im Bedarfsfall die verwendeten Prozeduren, um sich die für den Server verwendeten Werte in Erinnerung zu rufen.

Tabelle 12. Kompatibilität des IBM Spectrum Protect-Servers mit anderen Db2-Produkten auf dem System (Forts.)

Bedingung	Anweisungen
Ressourcenzuordnung	Sie müssen die Ressourcen und das Leistungsspektrum des Systems gegen die Anforderungen für den IBM Spectrum Protect-Server und die anderen Anwendungen, die das Db2-Produkt verwenden, abwägen. Damit den anderen Db2-Anwendungen genügend Ressourcen zur Verfügung stehen, müssen Sie unter Umständen die Einstellungen des IBM Spectrum Protect-Servers ändern, so dass der Server weniger Systemspeicher und -ressourcen verwendet. Wenn die Verarbeitungsprozesse für die anderen Db2-Anwendungen und der IBM Spectrum Protect-Server um Prozessor- und Speicherressourcen konkurrieren, kann die Leistung des Servers in Bezug auf die Verarbeitung der erwarteten Clientauslastung oder anderer Serveroperationen beeinträchtigt werden. Um die Ressourcen zu trennen und die Möglichkeit zur Optimierung und Zuordnung von Prozessor-, Speicher- und anderen Systemressourcen für mehrere Anwendungen zu verbessern, sollten Sie Unterstützung für logische Partitionen (LPAR), Auslastungspartitionierung (WPAR) oder andere Unterstützung für virtuelle Workstations einsetzen. Führen Sie eine Db2-Anwendung beispielsweise auf einem eigenen virtuellen System aus.

IBM Installation Manager

IBM Spectrum Protect verwendet IBM Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.

Wenn die erforderliche Version von IBM Installation Manager noch nicht installiert ist, wird sie automatisch installiert oder aktualisiert, wenn Sie IBM Spectrum Protect installieren. Die Software muss auf dem System installiert bleiben, damit IBM Spectrum Protect später nach Bedarf aktualisiert oder deinstalliert werden kann.

Die folgende Liste enthält Erläuterungen einiger Begriffe, die in IBM Installation Manager verwendet werden:

Angebot
Eine installierbare Einheit eines Softwareprodukts.

Das Angebot 'IBM Spectrum Protect' enthält alle Datenträger, die IBM Installation Manager für die Installation von IBM Spectrum Protect benötigt.

Paket
Die Gruppe der Softwarekomponenten, die für die Installation eines Angebots benötigt werden.

Das IBM Spectrum Protect-Paket enthält folgende Komponenten:

- Installationsprogramm IBM Installation Manager

- Das Angebot 'IBM Spectrum Protect'

Paketgruppe
Eine Gruppe von Paketen mit demselben übergeordneten Verzeichnis.

Die Standardpaketgruppe für das IBM Spectrum Protect-Paket ist `IBM Installation Manager`.

Repository
Ein ferner oder lokaler Speicherbereich für Daten und andere Anwendungsressourcen.

Das IBM Spectrum Protect-Paket wird in einem Repository in IBM Fix Central gespeichert.

Verzeichnis für gemeinsam genutzte Ressourcen
Ein Verzeichnis, das Softwaredateien oder Plug-ins enthält, die von Paketen gemeinsam genutzt werden.

In dem Verzeichnis für gemeinsam genutzte Ressourcen speichert IBM Installation Manager installationsbezogene Dateien, darunter Dateien, die für das Rollback zu einer vorherigen Version von IBM Spectrum Protect verwendet werden.

Arbeitsblätter für Planungsdetails für den Server

Sie können die Arbeitsblätter für die Planung der Größe und der Position des für den IBM Spectrum Protect-Server benötigten Speichers verwenden. Sie können darauf auch Namen und Benutzer-IDs aufzeichnen.

Element	Erforderlicher Speicherbereich	Anzahl der Verzeichnisse	Position der Verzeichnisse
Die Datenbank			
Aktive Protokolldatei			
Archivprotokoll			
Optional: Protokollspiegel für die aktive Protokolldatei			
Optional: Sekundäres Archivprotokoll (Übernahmeverzeichnis für Archivprotokolle)			

Element	Namen und Benutzer-IDs	Position
Die *Instanzbenutzer-ID* für den Server. Mit dieser ID starten Sie den IBM Spectrum Protect-Server und führen ihn aus.		

Element	Namen und Benutzer-IDs	Position
Das *Ausgangsverzeichnis* des Servers. In diesem Verzeichnis befindet sich die Instanzbenutzer-ID.		
Der Datenbankinstanzname		
Das *Instanzverzeichnis* für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien).		
Der Servername; verwenden Sie einen eindeutigen Namen für jeden Server.		

Kapazitätsplanung

Zur Kapazitätsplanung für IBM Spectrum Protect gehört die Verwaltung von Ressourcen wie z. B. die Datenbank, das Wiederherstellungsprotokoll und der Bereich für gemeinsam genutzte Ressourcen.

Vorbereitende Schritte

Sie müssen den Speicherbedarf für die Datenbank und das Wiederherstellungsprotokoll schätzen, um die Ressourcen als Teil der Kapazitätsplanung zu maximieren. Der verfügbare Speicherplatz für den Bereich für gemeinsam genutzte Ressourcen muss für jede Installation bzw. jedes Upgrade ausreichen.

Speicherbedarf für die Datenbank schätzen

Sie können den Speicherbedarf für die Datenbank auf der Basis der maximalen Anzahl Dateien schätzen, die sich gleichzeitig im Serverspeicher befinden können, oder auf der Basis der Speicherpoolkapazität.

Informationen zu diesem Vorgang

Anfänglich sollte mindestens 25 GB Speicherplatz in der Datenbank verwendet werden. Stellen Sie entsprechend Speicherplatz im Dateisystem bereit. Eine Datenbankgröße von 25 GB ist für eine Testumgebung oder eine Umgebung, die nur einen Speicherarchivmanager umfasst, ausreichend. Für einen Produktionsserver, der Clientlasten unterstützt, sollte die Datenbank größer sein. Wenn Sie Plattenspeicherpools (DISK) mit wahlfreiem Zugriff verwenden, ist mehr Datenbank- und Protokollspeicherbereich erforderlich als für Speicherpools mit sequenziellem Zugriff.

Die maximale Größe der IBM Spectrum Protect-Datenbank beträgt 8 TB.

Informationen zur Festlegung der Größe einer Datenbank in einer Produktionsumgebung, die auf der Anzahl Dateien und der Speicherpoolgröße basiert, enthalten die folgenden Abschnitte.

Speicherbedarf für die Datenbank auf der Basis der Anzahl Dateien schätzen

Wenn die maximale Anzahl Dateien, die sich zu einem bestimmten Zeitpunkt im Serverspeicher befinden, geschätzt werden kann, können Sie diese Zahl verwenden, um den Speicherbedarf für die Datenbank zu schätzen.

Informationen zu diesem Vorgang

Um den Speicherbedarf auf der Basis der maximalen Anzahl Dateien im Serverspeicher zu schätzen, verwenden Sie die folgenden Richtlinien:

- 600-1000 Byte für jede gespeicherte Version einer Datei einschließlich der Imagesicherungen.

  Einschränkung: Diese Richtlinie umfasst nicht den Speicherplatz, der während der Datendeduplizierung verwendet wird.
- 100-200 Byte für jede Datei im Cache, jede Kopienspeicherpooldatei, jede Datei im Pool für aktive Daten und jede deduplizierte Datei.
- Zusätzlicher Speicherbereich ist für die Datenbankoptimierung erforderlich, um variable Datenzugriffsmuster und die Server-Back-End-Verarbeitung von Daten zu unterstützen. Die Größe des zusätzlichen Speicherplatzes entspricht 50 % der Schätzung für die Gesamtanzahl Byte für Dateiobjekte.

In dem folgenden Beispiel für einen einzelnen Client basieren bei Berechnungen auf den Maximalwerten in den vorhergehenden Richtlinien. Bei den Beispielen wird die mögliche Verwendung der Dateiaggregation nicht berücksichtigt. Im Allgemeinen wird durch das Aggregieren kleiner Dateien der erforderliche Speicherplatz in der Datenbank reduziert. Die Dateiaggregation betrifft keine speicherverwalteten Dateien.

Vorgehensweise

1. Berechnen Sie die Anzahl Dateiversionen. Addieren Sie alle folgenden Werte, um die Anzahl Dateiversionen zu erhalten:
   a) Berechnen Sie die Anzahl gesicherter Dateien.
   Beispiel: Möglicherweise werden bis zu 500.000 Clientdateien gleichzeitig gesichert. In diesem Beispiel sind die Speichermaßnahmen so definiert, dass maximal drei Kopien gesicherter Dateien aufbewahrt werden:

   ```
   500.000 Dateien * 3 Kopien = 1.500.000 Dateien
   ```

   b) Berechnen Sie die Anzahl Archivierungsdateien.
   Beispiel: Bis zu 100.000 Clientdateien können archivierte Kopien sein.

   c) Berechnen Sie die Anzahl speicherverwalteter Dateien.
   Beispiel: Bis zu 200.000 Clientdateien können von Client-Workstations umgelagert werden.

   Bei Verwendung von 1000 Byte pro Datei beträgt der Gesamtspeicherplatz in der Datenbank, der für die zu dem Client gehörigen Dateien erforderlich ist, 1,8 GB:

   ```
   (1.500.000 + 100.000 + 200.000) * 1000 = 1,8 GB
   ```

2. Berechnen Sie die Anzahl Dateien im Cache, Kopienspeicherpooldateien, Dateien im Pool für aktive Daten und deduplizierter Dateien:
   a) Berechnen Sie die Anzahl der Cachekopien.
   Beispiel: In einem Plattenspeicherpool mit 5 GB Kapazität ist Caching aktiviert. Die obere Umlagerungsschwelle des Pools ist 90 % und die untere Umlagerungsschwelle ist 70 %. Das heißt 20 % des Plattenpools (oder 1 GB) wird von Cachedateien belegt.

   Wenn die durchschnittliche Dateigröße ungefähr 10 KB beträgt, enthält der Cache zu jedem beliebigen Zeitpunkt etwa 100.000 Dateien:

   ```
   100.000 Dateien * 200 Byte = 19 MB
   ```

   b) Berechnen Sie die Anzahl Kopienspeicherpooldateien.
   Alle primären Speicherpools werden im Kopienspeicherpool gesichert:

   ```
   (1.500.000 + 100.000 + 200.000) * 200 Byte = 343 MB
   ```

   c) Berechnen Sie die Anzahl Dateien im Speicherpool für aktive Daten.
   Alle aktiven Clientsicherungsdaten in primären Speicherpools werden in den Speicherpool für aktive Daten kopiert. Angenommen, es sind 500.000 Versionen der 1.500.000 Sicherungsdateien im primären Speicherpool aktiv:

   ```
   500.000 * 200 Byte = 95 MB
   ```

d) Berechnen Sie die Anzahl deduplizierter Dateien.
Angenommen, ein deduplizierter Speicherpool enthält 50.000 Dateien:

```
50.000 * 200 Byte = 10 MB
```

Auf der Basis der vorhergehenden Berechnungen sind etwa 0,5 GB zusätzlicher Speicherplatz in der Datenbank für die Cachedateien, die Kopienspeicherpooldateien, die Dateien im Pool für aktive Daten und die deduplizierten Dateien des Clients erforderlich.

3. Berechnen Sie den zusätzlichen Speicherplatz, der für die Datenbankoptimierung benötigt wird.
Um optimalen Datenzugriff und optimale Verwaltung durch den Server bereitzustellen, ist zusätzlicher Speicherplatz in der Datenbank erforderlich. Die Größe des zusätzlichen Speicherplatzes in der Datenbank beträgt 50 % des Gesamtspeicherbedarfs für Dateiobjekte.

```
(1,8 + 0,5) * 50 % = 1,2 GB
```

4. Die Gesamtgröße des für den Client erforderlichen Datenbankspeicherbereichs berechnen. Die Gesamtgröße beträgt ca. 3,5 GB:

```
1,8 + 0,5 + 1,2 = 3,5 GB
```

5. Berechnen Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist.
Wenn der Client, der in den vorhergehenden Berechnungen verwendet wurde, ein typischer Client ist und Sie beispielsweise über 500 Clients verfügen, können Sie den Gesamtspeicherplatz in der Datenbank, der für alle Clients erforderlich ist, mithilfe der folgenden Berechnung schätzen:

```
500 * 3,5 = 1,7 TB
```

Ergebnisse

Tipp: In den Beispielen oben handelt es sich bei den Ergebnissen um Schätzungen. Die tatsächliche Größe der Datenbank kann aufgrund von Faktoren wie beispielsweise der Anzahl Verzeichnisse und der Länge der Pfad- und Dateinamen von der geschätzten Größe abweichen. Sie sollten die Datenbank regelmäßig überwachen und die Größe wie erforderlich anpassen.

Nächste Schritte

Während des normalen Betriebs erfordert der IBM Spectrum Protect-Server möglicherweise temporären Speicherplatz in der Datenbank. Dieser Speicherplatz wird aus den folgenden Gründen benötigt:

- Zum Speichern der Ergebnisse der Sortierung oder Änderung der Reihenfolge, die noch nicht in der Datenbank aufbewahrt und in der Datenbank nicht unmittelbar optimiert werden. Die Ergebnisse werden vorübergehend in der Datenbank zur Verarbeitung gespeichert.
- Zum Erteilen des Verwaltungszugriffs auf die Datenbank über eine der folgenden Methoden:
  - Ein Db2-ODBC-Client (ODBC = Open Database Connectivity)
  - Ein Oracle-JDBC-Client (JDBC = Java Database Connectivity)
  - SQL (Structured Query Language) für den Server über die Befehlszeile eines Verwaltungsclients

Erwägen Sie die Verwendung von zusätzlichen 50 GB an temporärem Speicherplatz pro 500 GB Speicherbereich für Dateiobjekte und Optimierung. Siehe die Richtlinien in der folgenden Tabelle. In dem Beispiel, das im vorhergehenden Schritt verwendet wurde, sind insgesamt 1,7 TB Speicherplatz in der Datenbank für Dateiobjekte und die Optimierung für 500 Clients erforderlich. Auf der Basis dieser Berechnung sind 200 GB für temporären Speicherplatz erforderlich. Der erforderliche Gesamtspeicherplatz in der Datenbank beträgt 1,9 TB.

Datenbankgröße	Mindestens erforderlicher temporärer Speicherplatz
< 500 GB	50 GB

Datenbankgröße	Mindestens erforderlicher temporärer Speicherplatz
≥ 500 GB und < 1 TB	100 GB
≥ 1 TB und < 1,5 TB	150 GB
≥ 1,5 und < 2 TB	200 GB
≥ 2 und < 3 TB	250-300 GB
≥ 3 und < 4 TB	350-400 GB

Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität schätzen

Um den Speicherbedarf für die Datenbank auf der Basis der Speicherpoolkapazität zu schätzen, verwenden Sie ein Verhältnis von 1-5 %. Sind beispielsweise 200 TB Speicherpoolkapazität erforderlich, sollte die Größe der Datenbank erwartungsgemäß zwischen 2 und 10 TB betragen. Als allgemeine Regel gilt: Wählen Sie die Größe ihrer Datenbank so groß wie möglich, um zu verhindern, dass der Speicherplatz knapp wird. Wenn der Speicherplatz kapp wird, können Serveroperationen und Clientspeicheroperationen fehlschlagen.

Datenbankmanager und temporärer Speicherbereich

Der Datenbankmanager des IBM Spectrum Protect-Servers verwaltet Systemspeicher und Plattenspeicher für die Datenbank und ordnet diesen Speicher zu. Der benötigte Datenbankspeicherbereich ist von der Größe des verfügbaren Systemspeichers und von der Serverauslastung abhängig.

Der Datenbankmanager sortiert Daten in einer bestimmten Reihenfolge, gemäß der SQL-Anweisung, mit der Sie die Daten anfordern. Je nach Auslastung des Servers und wenn es mehr Daten gibt, als der Datenbankmanager verwalten kann, werden die (der Reihenfolge nach sortierten) Daten temporärem Plattenspeicher zugeordnet. Daten werden temporärem Plattenspeicher zugeordnet, wenn die Ergebnismenge sehr umfangreich ist. Der Datenbankmanager verwaltet den verwendeten Speicher dynamisch, wenn Daten temporärem Plattenspeicher zugeordnet werden.

Bei der Verfallsverarbeitung kann beispielsweise eine umfangreiche Ergebnismenge generiert werden. Wenn der Systemspeicher in der Datenbank zur Speicherung der Ergebnismenge nicht ausreicht, wird ein Teil der Daten temporärem Plattenspeicher zugeordnet. Wenn während der Verfallsverarbeitung ein Knoten oder ein Dateibereich ausgewählt wird, der für die Verarbeitung zu groß ist, kann der Datenbankmanager die Daten im Speicher nicht sortieren. Der Datenbankmanager muss temporären Speicherbereich zum Sortieren der Daten verwenden.

Bei der Ausführung von Datenbankoperationen sollten Sie in den folgenden Szenarios eine Erweiterung des Speicherplatzes in der Datenbank vornehmen:

- Der Speicherbereich der Datenbank ist klein und die Serveroperation, die temporären Speicherbereich benötigt, belegt den verbleibenden freien Speicherbereich.
- Die Dateibereiche sind groß oder den Dateibereichen ist eine Maßnahme zugeordnet, durch die viele Dateiversionen erstellt werden.
- Der IBM Spectrum Protect-Server muss mit begrenztem Speicher ausgeführt werden. Die Datenbank verwendet den Hauptspeicher des IBM Spectrum Protect-Servers für Datenbankoperationen. Ist der verfügbare Speicher jedoch nicht ausreichend, ordnet der IBM Spectrum Protect-Server der Datenbank temporären Speicherbereich auf Platte zu. Wenn beispielsweise 10G Speicher zur Verfügung stehen und Datenbankoperationen 12G Speicher benötigen, verwendet die Datenbank temporären Speicherbereich.
- Bei der Implementierung eines IBM Spectrum Protect-Servers wird ein Fehler aufgrund fehlenden Datenbankspeicherbereichs (`out of database space`) angezeigt. Überwachen Sie das Serveraktivitätenprotokoll auf Nachrichten, die sich auf den Datenbankspeicherbereich beziehen.

Wichtig: Sie dürfen die Db2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der Db2-Software und führen Sie kein Upgrade durch, um eine Beschädigung der Datenbank zu vermeiden.

Speicherplatzbedarf für das Wiederherstellungsprotokoll

In IBM Spectrum Protect beinhaltet der Begriff *Wiederherstellungsprotokoll* die aktive Protokolldatei, das Archivprotokoll, den Spiegel der aktiven Protokolldatei und das Archivübernahmeprotokoll. Der für das Wiederherstellungsprotokoll erforderliche Speicherbereich ist von verschiedenen Faktoren, wie z. B. dem Umfang der Clientaktivität mit dem Server, abhängig.

Speicherbereich für die aktive Protokolldatei und das Archivprotokoll

Wenn Sie den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll schätzen, müssen Sie einigen zusätzlichen Speicherbereich für gelegentlich auftretende hohe Lasten und Übernahmesituationen einkalkulieren.

In IBM Spectrum Protect-Servern der Version 7.1 und höher kann die aktive Protokolldatei eine maximale Größe von 512 GB haben. Die Größe des Archivprotokolls ist auf die Größe des Dateisystems beschränkt, in dem es installiert ist.

Berücksichtigen Sie bei der Schätzung der Größe der aktiven Protokolldatei die folgenden allgemeinen Richtlinien:

- Die empfohlene Anfangsgröße für die aktive Protokolldatei ist 16 GB.
- Stellen Sie sicher, das die aktive Protokolldatei mindestens groß genug ist, um die gleichzeitig ablaufende Aktivität handhaben zu können, die der Server in der Regel handhabt. Versuchen Sie als Vorsichtsmaßnahme das größte Arbeitsvolumen zu schätzen, das der Server jeweils handhabt. Stellen Sie für die aktive Protokolldatei zusätzlichen Speicherbereich bereit, der, falls erforderlich, verwendet werden kann. Ziehen Sie 20 % zusätzlichen Speicherbereich in Betracht.
- Überwachen Sie den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei. Passen Sie die Größe der aktiven Protokolldatei wie erforderlich abhängig von Faktoren wie Clientaktivität und Ebene der Serveroperationen an.
- Stellen Sie sicher, dass das Verzeichnis, das die aktive Protokolldatei enthält, mindestens genauso groß wie die aktive Protokolldatei ist. Ein Verzeichnis, das größer als die aktive Protokolldatei ist, kann Übernahmesituationen handhaben, sollten diese auftreten.
- Stellen Sie sicher, dass das Dateisystem, das das Verzeichnis für aktive Protokolldateien enthält, über mindestens 8 GB freien Speicherbereich für Anforderungen zum Versetzen temporärer Protokolle verfügt.

Die vorgeschlagene Anfangsgröße für das Archivprotokoll beträgt 48 GB.

Das Archivprotokollverzeichnis muss groß genug sein, um die Protokolldateien aufnehmen zu können, die seit der vorherigen Gesamtsicherung generiert wurden. Wenn Sie beispielsweise täglich eine Gesamtsicherung der Datenbank ausführen, muss das Archivprotokollverzeichnis groß genug sein, um die Protokolldateien für die gesamte Clientaktivität aufnehmen zu können, die während 24 Stunden stattfindet. Um Speicherbereich wiederherzustellen, löscht der Server veraltete Archivprotokolldateien nach einer Gesamtsicherung der Datenbank. Wenn das Archivprotokollverzeichnis voll wird und kein Verzeichnis für Archivübernahmeprotokolle vorhanden ist, verbleiben Protokolldateien im Verzeichnis für aktive Protokolldateien. Diese Bedingung kann zur Folge haben, dass das Verzeichnis für aktive Protokolldateien vollständig gefüllt und der Server gestoppt wird. Bei einem Serverneustart wird ein Teil des vorhandenen Speicherbereichs für die aktive Protokolldatei freigegeben wird.

Nach der Installation des Servers können Sie die Archivprotokollauslastung und den Speicherbereich im Archivprotokollverzeichnis überwachen. Wenn sich der Speicherbereich im Archivprotokollverzeichnis füllt, können die folgenden Probleme auftreten:

- Der Server kann keine Datenbankgesamtsicherungen ausführen. Untersuchen und beheben Sie dieses Problem.

- Andere Anwendungen schreiben in das Archivprotokollverzeichnis und belegen den für das Archivprotokoll erforderlichen Speicherbereich. Nutzen Sie den Speicherbereich für das Archivprotokoll nicht gemeinsam mit anderen Anwendungen, einschließlich anderer IBM Spectrum Protect-Server. Stellen Sie sicher, dass jeder Server über eine separate Speicherposition verfügt, dessen Eigner dieser spezifische Server ist und der von diesem spezifischen Server verwaltet wird.

Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen schätzen

Grundlegende Clientspeicheroperationen umfassen Sicherung, Archivierung und Speicherbereichsverwaltung. Der Protokollspeicherbereich muss groß genug sein, um alle Speichertransaktionen handhaben zu können, die gleichzeitig aktiv sind.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen zu bestimmen, führen Sie die folgende Berechnung aus:

```
Anzahl Clients  x  In jeder Transaktion gespeicherte Dateien
  x  Für jede Datei benötigter Protokollspeicherbereich
```

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 13. Grundlegende Clientspeicheroperationen

Element	Beispielwerte	Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3053 Byte	Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Aktive Protokolldatei: vorgeschlagene Größe	19,5 GB [1]	Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.
		`(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 Byte = 3,5 GB`
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
		`3,5 + 16 = 19,5 GB`

Tabelle 13. Grundlegende Clientspeicheroperationen (Forts.)

Element	Beispielwerte	Beschreibung

Archivprotokoll: vorgeschlagene Größe	58,5 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen.
		`3,5 x 3 = 10,5 GB`
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		`10,5 + 48 = 58,5 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, schätzen

Wenn Sie Clientoption RESOURCEUTILIZATION auf einen größeren Wert als den Standardwert gesetzt ist, erhöht sich die gleichzeitige Last für den Server.

Um die Größe der aktiven Protokolldatei und des Archivprotokolls für Clients, die mehrere Sitzungen verwenden, zu bestimmen, führen Sie die folgende Berechnung aus:

```
Anzahl Clients x Anzahl Sitzungen pro Client x Anzahl während
  jeder Transaktion gespeicherter Dateien x pro Datei erforderlicher
  Protokollspeicherbereich
```

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 14. Mehrere Clientsitzungen

Element	Beispielwerte		Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	1000	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Mögliche Sitzungen für jeden Client	3	3	Die Einstellung der Clientoption RESOURCEUTILIZATION ist größer als der Standardwert. Jede Clientsitzung führt maximal drei Sitzungen parallel aus.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.

Tabelle 14. Mehrere Clientsitzungen (Forts.)

Element	**Beispielwerte**		**Beschreibung**
Für jede Datei erforderlicher Protokollspeicherbereich	3053	3053	Der Wert von 3053 Byte für jede Datei in einer Transaktion gibt die Protokollbyte an, die erforderlich sind, wenn Dateien von einem Windows-Client gesichert werden, auf dem Dateinamen eine Länge von 12-120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Aktive Protokolldatei: vorgeschlagene Größe	26,5 GB [1]	51 GB [1]	Die folgende Berechnung wurde für 300 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.
			`(300 Clients x 3 Sitzungen pro Client x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 = 10,5 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			`10,5 + 16 = 26,5 GB`
			Die folgende Berechnung wurde für 1000 Clients ausgeführt. 1 Gigabyte entspricht 1.073.741.824 Byte.
			`(1000 Clients x 3 Sitzungen pro Client x 4096 während jeder Transaktion gespeicherte Dateien x 3053 Byte pro Datei) ÷ 1.073.741.824 = 35 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			`35 + 16 = 51 GB`

Archivprotokoll: vorgeschlagene Größe	79,5 GB [1]	153 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, wird die Schätzung für die aktive Protokolldatei mit 3 multipliziert:
			`10,5 x 3 = 31,5 GB`
			`35 x 3 = 105 GB`
			Erhöhen Sie diese Werte um die vorgeschlagene Anfangsgröße von 48 GB:
			`31,5 + 48 = 79,5 GB`
			`105 + 48 = 153 GB`

Tabelle 14. Mehrere Clientsitzungen (Forts.)

Element	Beispielwerte	Beschreibung
[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen. Überwachen Sie Ihre aktive Protokolldatei und passen Sie die Größe, falls erforderlich, an.		

Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Operationen für gleichzeitiges Schreiben schätzen

Wenn Clientsicherungsoperationen Speicherpools verwenden, die für gleichzeitiges Schreiben konfiguriert sind, erhöht sich der Protokollspeicherbedarf, der für jede Datei erforderlich ist.

Der Protokollspeicherbereich, der für jede Datei erforderlich ist, erhöht sich um ungefähr 200 Byte für jeden Kopienspeicherpool, der für eine Operation für gleichzeitiges Schreiben verwendet wird. In dem Beispiel in der folgenden Tabelle werden Daten in einem primären Speicherpool und darüber hinaus in zwei Kopienspeicherpools gespeichert. Die geschätzte Protokollgröße erhöht sich für jede Datei um 400 Byte. Wenn Sie den vorgeschlagenen Wert von 3053 Byte Protokollspeicherbereich pro Datei verwenden, sind insgesamt 3453 Byte erforderlich.

Diese Berechnung wird in dem Beispiel in der folgenden Tabelle verwendet.

Tabelle 15. Operationen für gleichzeitiges Schreiben

Element	Beispielwerte	Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3453 Byte	3053 Byte plus 200 Byte für jeden Kopienspeicherpool. Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients für Sichern/Archivieren gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Tabelle 15. Operationen für gleichzeitiges Schreiben (Forts.)

Element	Beispiel-werte	Beschreibung

Aktive Protokolldatei: vorgeschlagene Größe	20 GB [1]	Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.
		`(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3453 Byte pro Datei) ÷ 1.073.741.824 Byte = 4,0 GB`
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
		`4 + 16 = 20 GB`

Archivprotokoll: vorgeschlagene Größe	60 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Speicherbedarf für das Archivprotokoll zu schätzen:
		`4 GB x 3 = 12 GB`
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		`12 + 48 = 60 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für grundlegende Clientspeicheroperationen und Serveroperationen schätzen

Die Umlagerung von Daten in Serverspeicher, Identifikationsprozesse für die Datendeduplizierung, Konsolidierung und Verfallsverarbeitung werden möglicherweise gleichzeitig mit Clientspeicheroperationen ausgeführt. Verwaltungstasks wie Verwaltungsbefehle oder SQL-Abfragen von Verwaltungsclients können ebenfalls gleichzeitig mit Clientspeicheroperationen ausgeführt werden. Serveroperationen und Verwaltungstasks, die gleichzeitig ausgeführt werden, können den erforderlichen Speicherbereich für die aktive Protokolldatei erhöhen.

Beispielsweise wird bei der Umlagerung von Dateien aus dem Speicherpool mit wahlfreiem Zugriff (DISK) in einem Plattenspeicherpool mit sequenziellem Zugriff (FILE) für jede Datei, die umgelagert wird, ungefähr 110 Byte Protokollspeicherbereich verwendet. Beispiel: Angenommen, es sind 300 Clients für Sichern/Archivieren vorhanden, von denen jeder 100.000 Dateien jede Nacht sichert. Die Dateien sind anfänglich in einem DISK-Speicherpool gespeichert und werden dann in einen FILE-Speicherpool umgelagert. Um die Größe des Speicherbereichs für die aktive Protokolldatei zu schätzen, die für die Datenumlagerung erforderlich ist, verwenden Sie die folgende Berechnung. Die Anzahl Clients in der Berechnung stellt die maximale Anzahl zu einem beliebigen Zeitpunkt dar, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern.

```
300 Clients x 100.000 Dateien pro Client x 110 Byte = 3,1 GB
```

Addieren Sie diesen Wert zu der Schätzung für die Größe der aktiven Protokolldatei, die für grundlegende Clientspeicheroperationen berechnet wurde.

Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls unter Bedingungen mit extremen Abweichungen schätzen

Probleme in Bezug auf knapp werdenden Speicherbereich für die aktive Protokolldatei können auftreten, wenn viele Transaktionen, die sehr schnell ausgeführt werden, zusammen mit einigen Transaktionen vorhanden sind, deren Ausführung sehr viel länger dauern kann. Ein typischer Fall sind viele aktive Workstation- oder Dateiserversicherungssitzungen und wenige aktive Serversicherungssitzungen für sehr große Datenbanken. Trifft diese Situation für Ihre Umgebung zu, müssen Sie möglicherweise die Größe der aktiven Protokolldatei erhöhen, damit die Arbeit erfolgreich ausgeführt werden kann.

Beispiel: Größe des Archivprotokolls bei Datenbankgesamtsicherungen schätzen

Der IBM Spectrum Protect-Server löscht nicht benötigte Dateien nur dann aus dem Archivprotokoll, wenn eine Datenbankgesamtsicherung ausgeführt wird. Demzufolge müssen Sie beim Schätzen des für das Archivprotokoll erforderlichen Speicherbereichs auch die Häufigkeit, mit der Datenbankgesamtsicherungen ausgeführt werden, berücksichtigen.

Wenn beispielsweise einmal pro Woche eine Datenbankgesamtsicherung ausgeführt wird, muss der Speicherbereich für das Archivprotokoll groß genug sein, um die Informationen einer vollständigen Woche im Archivprotokoll aufnehmen zu können.

Die unterschiedliche Größe des Archivprotokolls für täglich ausgeführte Datenbankgesamtsicherungen wird in dem Beispiel in der folgenden Tabelle gezeigt.

Tabelle 16. Datenbankgesamtsicherungen

Element	Beispielwerte	Beschreibung
Maximale Anzahl Clientknoten, die zu einem beliebigen Zeitpunkt gleichzeitig Dateien sichern, archivieren oder umlagern	300	Die Anzahl Clientknoten, die jede Nacht Dateien sichern, archivieren oder umlagern.
Anzahl während jeder Transaktion gespeicherter Dateien	4096	Der Standardwert für die Serveroption TXNGROUPMAX ist 4096.
Für jede Datei erforderlicher Protokollspeicherbereich	3453 Byte	3053 Byte für jede Datei plus 200 Byte für jeden Kopienspeicherpool. Der Wert von 3053 Byte für jede Datei in einer Transaktion stellt die Anzahl der Protokollbyte dar, die bei der Sicherung von Dateien auf einem Windows-Client benötigt werden, wo die Dateinamen 12 - 120 Byte haben. Dieser Wert basiert auf den Ergebnissen von Tests, die unter Laborbedingungen ausgeführt wurden. Bei den Tests wurde mit Clients gearbeitet, die Sicherungsoperationen in einen Plattenspeicherpool (DISK) mit wahlfreiem Zugriff ausführten. Plattenpools haben eine stärkere Protokollnutzung als Speicherpools mit sequenziellem Zugriff zur Folge. Wenn die Daten, die gespeichert werden, Dateinamen mit einer Länge von über 12-120 Byte haben, sollten Sie von einem Wert ausgehen, der 3053 Byte überschreitet.

Tabelle 16. Datenbankgesamtsicherungen (Forts.)

Element	Beispiel-werte	Beschreibung

Aktive Protokolldatei: vorgeschlagene Größe	20 GB [1]	Bestimmen Sie mithilfe der folgenden Berechnung die Größe der aktiven Protokolldatei. 1 Gigabyte entspricht 1.073.741.824 Byte.
		`(300 Clients x 4096 während jeder Transaktion gespeicherte Dateien x 3453 Byte pro Datei) ÷ 1.073.741.824 Byte = 4,0 GB`
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
		`4 + 16 = 20 GB`

Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamtsicherung pro Tag	60 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Sicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen:
		`4 GB x 3 = 12 GB`
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		`12 + 48 = 60 GB`

Archivprotokoll: vorgeschlagene Größe bei einer Datenbankgesamtsicherung pro Woche	132 GB [1]	Aufgrund der Voraussetzung, dass Archivprotokolle über drei Serverdatenbanksicherungszyklen hinweg speicherbar sein müssen, multiplizieren Sie die Schätzung für die aktive Protokolldatei mit 3, um den Gesamtspeicherbedarf für das Archivprotokoll zu schätzen. Multiplizieren Sie das Ergebnis mit der Anzahl Tage, die zwischen Datenbankgesamtsicherungen liegen.
		`(4 GB x 3 ) x 7 = 84 GB`
		Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
		`84 + 48 = 132 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 16 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Anfangsgröße für ein Archivprotokoll in einer Produktionsumgebung, die keine Deduplizierung verwendet, ist 48 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 16 GB bzw. 48 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

Beispiel: Größe der aktiven Protokolldatei und des Archivprotokolls für Datendeduplizierungsoperationen schätzen

Wenn Sie Daten deduplizieren, müssen Sie die Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll berücksichtigen.

Die folgenden Faktoren haben Auswirkungen auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll:

Volumen der deduplizierten Daten

Welche Auswirkungen die Datendeduplizierung auf den Speicherbedarf für die aktive Protokolldatei und das Archivprotokoll hat, ist von dem Prozentsatz an Daten abhängig, der für die Deduplizierung auswählbar ist. Ist der Prozentsatz an Daten, die dedupliziert werden können, relativ hoch, ist mehr Protokollspeicherbereich erforderlich.

Größe und Anzahl Speicherbereiche

Für jeden Speicherbereich, der durch einen Prozess zum Identifizieren doppelter Daten identifiziert wird, sind ungefähr 1.500 Byte Speicherbereich für die aktive Protokolldatei erforderlich. Werden beispielsweise 250.000 Speicherbereiche durch einen erkennen identifiziert, beträgt die geschätzte Größe der aktiven Protokolldatei 358 MB:

```
250.000 während jedes Prozesses ermittelte Speicherbereiche x 1.500 Byte
 für jeden Speicherbereich = 358 MB
```

Betrachten Sie das folgende Szenario. 300 Clients für Sichern/Archivieren sichern jede Nacht bis zu 100.000 Dateien. Diese Aktivität hat eine Last von 30.000.000 Dateien zur Folge. Die durchschnittliche Anzahl Speicherbereiche für jede Datei ist 2. Demzufolge beträgt die Gesamtzahl Speicherbereiche 60.000.000 und der Speicherbedarf für das Archivprotokoll 84 GB:

```
60.000.000 Speicherbereiche x 1.500 Byte pro Speicherbereich = 84 GB
```

Ein Prozess zum Identifizieren doppelter Daten wird für Aggregate von Dateien ausgeführt. Ein Aggregat besteht aus Dateien, die in einer bestimmten Transaktion gespeichert sind, wie durch die Serveroption TXNGROUPMAX angegeben. Angenommen, die Serveroption TXNGROUPMAX ist auf den Standardwert 4096 gesetzt. Wenn die durchschnittliche Anzahl Speicherbereiche für jede Datei 2 beträgt, ist die Gesamtzahl Speicherbereiche in jedem Aggregat 8192 und der für die aktive Protokolldatei erforderliche Speicherbedarf 12 MB:

```
8192 Speicherbereiche in jedem Aggregat x 1500 Byte pro Speicherbereich =
   12 MB
```

Timing und Anzahl der Prozesse zum Identifizieren doppelter Daten

Das Timing und die Anzahl Prozesse zum Identifizieren doppelter Daten haben ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei. Bei Verwendung der in dem vorhergehenden Beispiel berechneten Größe der aktiven Protokolldatei von 12 MB beträgt die gleichzeitige Last für die aktive Protokolldatei 120 MB, wenn 10 Prozesse zum Identifizieren doppelter Daten parallel ausgeführt werden:

```
12 MB pro Prozess x 10 Prozesse = 120 MB
```

Dateigröße

Große Dateien, die für die Identifizierung doppelter Daten verarbeitet werden, können ebenfalls Auswirkungen auf die Größe der aktiven Protokolldatei haben. Beispiel: Angenommen, ein Client für Sichern/Archivieren sichert ein Dateisystemimage mit einer Größe von 80 GB. Die Anzahl doppelter Speicherbereiche für dieses Objekt kann groß sein, wenn beispielsweise die in das Dateisystemimage eingeschlossenen Dateien mit Teilsicherungen gesichert wurden. Beispiel: Angenommen, ein Dateisystemimage hat 1,2 Millionen doppelte Speicherbereiche. Die 1,2 Millionen Speicherbereiche in dieser großen Datei stellen eine einzige Transaktion für einen Prozess zum Identifizieren doppelter Daten dar. Der Gesamtspeicherbereich in der aktiven Protokolldatei, der für dieses einzelne Objekt erforderlich ist, beträgt 1,7 GB:

```
1.200.000 Speicherbereich x 1.500 Byte pro Speicherbereich = 1,7 GB
```

Wenn andere, kleinere Prozesse zum Identifizieren doppelter Daten zu demselben Zeitpunkt ausgeführt werden wie der Prozess zum Identifizieren doppelter Daten für ein einzelnes großes Objekt, ist in der aktiven Protokolldatei möglicherweise nicht genügend Speicherbereich verfügbar. Beispiel: Angenommen, ein Speicherpool ist für die Deduplizierung aktiviert. Der Speicherpool enthält gemischte Daten, einschließlich vieler relativ kleiner Dateien mit einer Größe von 10 KB bis zu mehreren hundert KB. Der Speicherpool enthält außerdem einige wenige große Objekte mit einem hohen Prozentsatz an doppelten Speicherbereichen.

Um nicht nur den Speicherbedarf zu berücksichtigen, sondern auch das Timing und die Dauer gleichzeitig ablaufender Transaktionen, erhöhen Sie die geschätzte Größe der aktiven Protokolldatei um den Faktor 2. Beispiel: Angenommen, das Ergebnis Ihrer Berechnungen für den Speicherbedarf lautet 25 GB (23,3 GB + 1,7 GB für die Deduplizierung eines großen Objekts). Wenn Deduplizierungsverarbeitung gleichzeitig ausgeführt werden, beträgt die vorgeschlagene Größe der aktiven Protokolldatei 50 GB. Die vorgeschlagene Größe des Archivprotokolls ist 150 GB.

Die Beispiele in den folgenden Tabellen zeigen Berechnungen für aktive Protokolldateien und Archivprotokolle. In dem Beispiel in der ersten Tabelle wird eine durchschnittliche Größe von 700 KB für Speicherbereiche verwendet. In dem Beispiel in der zweiten Tabelle wird eine durchschnittliche Größe von 256 KB verwendet. Wie den Beispielen zu entnehmen ist, zeigt die durchschnittliche Größe doppelter Speicherbereiche von 256 KB eine größere geschätzte Größe für die aktive Protokolldatei an. Um betriebsbezogene Probleme für den Server auf ein Mindestmaß reduzieren oder zu verhindern, verwenden Sie 256 KB für die Schätzung der Größe der aktiven Protokolldatei in Ihrer Produktionsumgebung.

Tabelle 17. Durchschnittliche Größe doppelter Speicherbereiche von 700 KB

Element	**Beispielwerte**		**Beschreibung**
Größe des größten zu deduplizierenden Objekts	800 GB	4 TB	Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar.
Durchschnittliche Größe der Speicherbereiche	700 KB	700 KB	Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.
Speicherbereiche für eine bestimmte Datei	1.198.372 Bit	6.135.667 Bit	Bei Verwendung der durchschnittlichen Speicherbereichsgröße (700 KB), geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an. Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt: `(800 GB ÷ 700 KB) = 1.198.372 Bit` Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt: `(4 TB ÷ 700 KB) = 6.135.667 Bit`
Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist	1,7 GB	8,6 GB	Der geschätzte Speicherbereich für die aktive Protokolldatei, der für diese Transaktion benötigt wird.

Tabelle 17. Durchschnittliche Größe doppelter Speicherbereiche von 700 KB (Forts.)

Element	Beispielwerte		Beschreibung

Aktive Protokolldatei: vorgeschlagene Gesamtgröße	66 GB [1]	79,8 GB [1]	Multiplizieren Sie, nachdem zusätzlich zur Deduplizierung andere Aspekte der Last auf dem Server berücksichtigt wurden, die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			`(23,3 GB + 1,7 GB) x 2 = 50 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			`50 + 16 = 66 GB`
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			`(23,3 GB + 8,6 GB) x 2 = 63,8 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			`63,8 + 16 = 79,8 GB`

Archivprotokoll: vorgeschlagene Größe	198 GB [1]	239,4 GB [1]	Multiplizieren Sie die geschätzte Größe der aktiven Protokolldatei mit dem Faktor 3.
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			`50 GB x 3 = 150 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			`150 + 48 = 198 GB`
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			`63,8 GB x 3 = 191,4 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			`191,4 + 48 = 239,4 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

Tabelle 18. Durchschnittliche Größe doppelter Speicherbereiche von 256 KB

Element	**Beispielwerte**		**Beschreibung**
Größe des größten zu deduplizierenden Objekts	800 GB	4 TB	Die Granularität der Verarbeitung für die Deduplizierung bezieht sich auf die Dateiebene. Demzufolge stellt die größte einzelne zu deduplizierende Datei die umfangreichste Transaktion und eine entsprechend hohe Last für die aktive Protokolldatei und das Archivprotokoll dar.
Durchschnittliche Größe der Speicherbereiche	256 KB	256 KB	Die Deduplizierungsalgorithmen verwenden eine variable Blockmethode. Nicht alle deduplizierten Speicherbereiche für eine bestimmte Datei haben dieselbe Größe, daher wird bei dieser Berechnung eine durchschnittliche Speicherbereichsgröße vorausgesetzt.

Speicherbereiche für eine bestimmte Datei	3.276.800 Bit	16.777.216 Bit	Bei Verwendung der durchschnittlichen Speicherbereichsgröße, geben diese Berechnungen die Gesamtzahl Speicherbereiche für ein bestimmtes Objekt an.
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			`(800 GB ÷ 256 KB) = 3.276.800 Bit`
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			`(4 TB ÷ 256 KB) = 16.777.216 Bit`

Aktive Protokolldatei: vorgeschlagene Größe, die für die Deduplizierung eines einzelnen großen Objekts während eines einzelnen Prozesses zum Identifizieren doppelter Daten erforderlich ist	4,5 GB	23,4 GB	Die geschätzte Größe des Speicherbereichs für die aktive Protokolldatei, die für diese Transaktion erforderlich ist.

Tabelle 18. Durchschnittliche Größe doppelter Speicherbereiche von 256 KB (Forts.)

Element	Beispielwerte		Beschreibung

Aktive Protokolldatei: vorgeschlagene Gesamtgröße	71,6 GB [1]	109,4 GB [1]	Nachdem Sie neben der Deduplizierung andere Aspekte der Serverauslastung mit berücksichtigt haben, multiplizieren Sie die vorhandene Schätzung mit dem Faktor 2. In diesen Beispielen wird der zum Deduplizieren eines einzelnen großen Objekts erforderliche Speicherbereich für die aktive Protokolldatei im Zusammenhang mit den vorherigen Schätzungen für die erforderliche Größe der aktiven Protokolldatei betrachtet.
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit einer Größe von 800 GB ausgeführt:
			`(23,3 GB + 4,5 GB) x 2 = 55,6 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			`55,6 + 16 = 71,6 GB`
			Die folgende Berechnung wurde für mehrere Transaktionen und ein Objekt mit 4 TB verwendet:
			`(23,3 GB + 23,4 GB) x 2 = 93,4 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 16 GB:
			`93,4 + 16 = 109,4 GB`

Archivprotokoll: vorgeschlagene Größe	214,8 GB [1]	328,2 GB [1]	Die geschätzte Größe der aktiven Protokolldatei multipliziert mit dem Faktor 3.
			Die folgende Berechnung wurde für ein Objekt mit einer Größe von 800 GB ausgeführt:
			`55,6 GB x 3 = 166,8 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			`166,8 + 48 = 214,8 GB`
			Die folgende Berechnung wurde für ein Objekt mit einer Größe von 4 TB ausgeführt:
			`93,4 GB x 3 = 280,2 GB`
			Erhöhen Sie diesen Wert um die vorgeschlagene Anfangsgröße von 48 GB:
			`280,2 + 48 = 328,2 GB`

[1] Die Beispielwerte in dieser Tabelle zeigen, wie die Größe für die aktive Protokolldatei und das Archivprotokoll berechnet werden. In einer Produktionsumgebung, die die Deduplizierung verwendet, ist 32 GB die vorgeschlagene Mindestgröße für eine aktive Protokolldatei. Die vorgeschlagene Mindestgröße für ein Archivprotokoll in einer Produktionsumgebung, die die Deduplizierung verwendet, ist 96 GB. Wenn Sie die Werte durch Werte aus Ihrer Umgebung ersetzen und die Ergebnisse 32 GB bzw. 96 GB überschreiten, verwenden Sie Ihre Ergebnisse, um die Größe der aktiven Protokolldatei und des Archivprotokolls zu berechnen.

Überwachen Sie Ihre Protokolle und passen Sie die Größe, falls erforderlich, an.

Speicherbereich des Spiegels für aktive Protokolldateien

Die aktive Protokolldatei kann gespiegelt werden, sodass die gespiegelte Kopie verwendet werden kann, falls die aktiven Protokolldateien nicht gelesen werden können. Es kann nur ein einziger Spiegel der aktiven Protokolldatei vorhanden sein.

Die Erstellung einer Protokollspiegel ist eine vorgeschlagene Option. Wenn Sie die aktive Protokolldatei vergrößern, wird der Protokollspiegel automatisch vergrößert. Die Spiegelung des Protokolls kann sich negativ auf die Leistung auswirken, da die doppelte E/A-Aktivität erforderlich ist, um den Spiegel zu verwalten. Der zusätzliche Speicherbereich, den der Protokollspiegel benötigt, ist ein weiterer Faktor, der bei der Entscheidung über die Erstellung eines Protokollspiegels berücksichtigt werden muss.

Wenn das Spiegelprotokollverzeichnis voll wird, gibt der Server Fehlernachrichten in das Aktivitätenprotokoll und in die Datei `db2diag.log` aus. Die Serveraktivität wird fortgesetzt.

Speicherbereich des Übernahmeverzeichnisses für Archivprotokolle

Das Übernahmeverzeichnis für Archivprotokolle wird vom Server verwendet, wenn der Speicherbereich des Verzeichnisses für Archivprotokolle nicht mehr ausreicht.

Durch Angabe eines Übernahmeverzeichnisses für Archivprotokolle können Probleme verhindert werden, die auftreten, wenn der Speicherbereich der Archivprotokolldatei nicht mehr ausreicht. Wenn sowohl das Verzeichnis für Archivprotokolle als auch das Laufwerk oder das Dateisystem, in dem sich das Übernahmeverzeichnis für Archivprotokolle befindet, voll wird, bleiben die Daten im Verzeichnis für aktive Protokolldateien. Dadurch kann die aktive Protokolldatei vollständig ausgefüllt werden, was einen Serverhalt verursacht.

Speicherauslastung für die Datenbank und die Wiederherstellungsprotokolle überwachen

Um den belegten und verfügbaren Speicherbereich für die aktive Protokolldatei zu bestimmen, geben Sie den Befehl **QUERY LOG** ein. Um die Speicherauslastung in der Datenbank und den Wiederherstellungsprotokollen zu überwachen, können Sie auch das Aktivitätenprotokoll auf Nachrichten überprüfen.

Aktive Protokolldatei

Wenn der verfügbare Speicherbereich für die aktive Protokolldatei zu gering ist, werden die folgenden Nachrichten im Aktivitätenprotokoll angezeigt:

ANR4531I: IC_AUTOBACKUP_LOG_USED_SINCE_LAST_BACKUP_TRIGGER
Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Der IBM Spectrum Protect-Server startet eine Datenbankgesamtsicherung.

Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei `dsmserv.opt` und geben Sie für die Option `ACTIVELOGSIZE` einen neuen Wert an. Starten Sie anschließend den Server erneut.

ANR0297I: IC_BACKUP_NEEDED_LOG_USED_SINCE_LAST_BACKUP
Diese Nachricht wird angezeigt, wenn der Speicherbereich für die aktive Protokolldatei die angegebene maximale Größe überschreitet. Sie müssen die Datenbank manuell sichern.

Um die maximale Protokollgröße zu ändern, stoppen Sie den Server. Öffnen Sie die Datei `dsmserv.opt` und geben Sie für die Option `ACTIVELOGSIZE` einen neuen Wert an. Starten Sie anschließend den Server erneut.

ANR4529I: IC_AUTOBACKUP_LOG_UTILIZATION_TRIGGER
Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Wenn mindestens eine einzige Datenbankgesamtsicherung ausgeführt wurde, startet der IBM Spectrum Protect-Server eine Teilsicherung der Datenbank. Andernfalls startet der Server eine Datenbankgesamtsicherung.

ANR0295I: IC_BACKUP_NEEDED_LOG_UTILIZATION
Das Verhältnis des belegten Speicherbereichs für die aktive Protokolldatei zum verfügbaren Speicherbereich für die aktive Protokolldatei überschreitet den Schwellenwert für die Protokollauslastung. Sie müssen die Datenbank manuell sichern.

Archivprotokoll

Wenn der verfügbare Speicherbereich für das Archivprotokoll zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

ANR0299I: IC_BACKUP_NEEDED_ARCHLOG_USED
Das Verhältnis des belegten Speicherbereichs für das Archivprotokoll zum verfügbaren Speicherbereich für das Archivprotokoll überschreitet den Schwellenwert für die Protokollauslastung. Der IBM Spectrum Protect-Server startet eine automatische Datenbankgesamtsicherung.

Datenbank

Wenn der verfügbare Speicherbereich für Datenbankaktivitäten zu gering ist, wird die folgende Nachricht im Aktivitätenprotokoll angezeigt:

ANR2992W: IC_LOG_FILE_SYSTEM_UTILIZATION_WARNING_2
Der belegte Speicherplatz in der Datenbank überschreitet den Schwellenwert für die Belegung des Speicherplatzes in der Datenbank. Um den Speicherplatz für die Datenbank zu vergrößern, verwenden Sie den Befehl **EXTEND DBSPACE** oder das Dienstprogramm **DSMSERV FORMAT** mit dem Parameter **DBDIR**.

ANR1546W: FILESYSTEM_DBPATH_LESS_1GB
Der verfügbare Speicherbereich in dem Verzeichnis, in dem sich die Serverdatenbankdateien befinden, beträgt weniger als 1 GB.

Wenn ein IBM Spectrum Protect-Server mit dem Dienstprogramm DSMSERV FORMAT oder dem Konfigurationsassistenten erstellt wird, werden auch eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien erstellt, in denen Datenbankinformationen gespeichert werden sollen, die vom Datenbankmanager verwendet werden. Der in dieser Nachricht angegebene Pfad gibt die Speicherposition der Datenbankinformationen an, die vom Datenbankmanager verwendet werden. Ist in dem Pfad kein Speicherbereich verfügbar, ist der Server nicht mehr funktionsfähig.

Sie müssen dem Dateisystem Speicherbereich hinzufügen oder in dem Dateisystem oder auf der Platte Speicherbereich freigeben.

Rollbackdateien der Installation löschen

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, löschen, um Speicherplatz im Verzeichnis für gemeinsam genutzte Ressourcen freizugeben. Zu den Dateitypen, die Sie löschen können, gehören z. B. Dateien, die für eine Rollbackoperation benötigt wurden.

Informationen zu diesem Vorgang

Zum Löschen der nicht mehr benötigten Dateien verwenden Sie den grafisch orientierten Installationsassistenten oder die Befehlszeile im Konsolenmodus.

Rollbackdateien für die Installation mit einem grafisch orientierten Assistenten löschen

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der IBM Installation Manager-Benutzerschnittstelle löschen.

Vorgehensweise

1. Öffnen Sie IBM Installation Manager.

In dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis `eclipse` (z. B. `/opt/IBM/InstallationManager/eclipse`) und geben Sie folgenden Befehl aus, um IBM Installation Manager zu starten:

```
./IBMIM
```

2. Klicken Sie auf **Datei** > **Benutzervorgaben**.
3. Wählen Sie **Dateien für Rollback** aus.
4. Klicken Sie auf **Gespeicherte Dateien löschen** und dann auf **OK**.

Rollbackdateien für die Installation mit der Befehlszeile löschen

Sie können bestimmte Installationsdateien, die während des Installationsprozesses gespeichert wurden, mithilfe der Befehlszeile löschen.

Vorgehensweise

1. In dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:

   `eclipse/tools`

   Beispiel:

   `/opt/IBM/InstallationManager/eclipse/tools`
2. Geben Sie im Verzeichnis `tools` den folgenden Befehl aus, um eine IBM Installation Manager-Befehlszeile zu starten:

   `./imcl -c`
3. Geben Sie P ein, um **Benutzervorgaben** auszuwählen.
4. Geben Sie 3 ein, um **Dateien für Rollback** auszuwählen.
5. Geben Sie D ein, um die **Dateien für Rollback** zu **löschen**.
6. Geben Sie A ein, um die **Änderungen anzuwenden und zum Benutzervorgabenmenü zurückzukehren**.
7. Geben Sie C ein, um das **Benutzervorgabenmenü** zu verlassen.
8. Geben Sie X ein, um **Installation Manager zu beenden**.

Empfehlungen für die Serverbenennung

Verwenden Sie diese Beschreibungen als Referenz bei der Installation oder beim Upgrade eines IBM Spectrum Protect-Servers.

Instanzbenutzer-ID

Die Instanzbenutzer-ID wird als Basis für andere Namen verwendet, die sich auf die Serverinstanz beziehen. Die Instanzbenutzer-ID wird auch als Instanzeigner bezeichnet.

Zum Beispiel: tsminst1

Die Instanzbenutzer-ID ist die Benutzer-ID, die über das Eigentumsrecht oder über Schreib-/Lesezugriffsberechtigung für alle Verzeichnisse verfügen muss, die Sie für die Datenbank und das Wiederherstellungsprotokoll erstellen. Der Server wird standardmäßig mit der Instanzbenutzer-ID ausgeführt. Diese Benutzer-ID benötigt außerdem Schreib-/Lesezugriff für die Verzeichnisse, die für die Einheitenklasse **FILE** verwendet werden.

Ausgangsverzeichnis für die Instanzbenutzer-ID

Das Ausgangsverzeichnis kann während der Erstellung der Instanzbenutzer-ID erstellt werden. Hierfür wird die Option für die Erstellung eines Ausgangsverzeichnisses (`-m`) verwendet, falls es noch nicht

vorhanden ist. Abhängig von den lokalen Einstellungen kann das Verzeichnis folgendes Format haben: /home/*Instanzbenutzer-ID*

Zum Beispiel: /home/tsminst1

Das Ausgangsverzeichnis dient hauptsächlich zur Aufbewahrung des Profils für die Benutzer-ID und für Sicherheitseinstellungen.

Datenbankinstanzname

Der Datenbankinstanzname muss mit der Instanzbenutzer-ID identisch sein, mit der Sie die Serverinstanz ausführen.

Zum Beispiel: tsminst1

Instanzverzeichnis

Das Instanzverzeichnis enthält spezielle Dateien für eine Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien). Es kann einen beliebigen Name haben. Um die Identifizierung zu erleichtern, sollten Sie einen Namen verwenden, der das Verzeichnis mit dem Instanznamen verknüpft.

Sie können das Instanzverzeichnis als Unterverzeichnis des Ausgangsverzeichnisses für die Instanzbenutzer-ID erstellen. Zum Beispiel: /home/*Instanzbenutzer-ID*/*Instanzbenutzer-ID*

Im folgenden Beispiel befindet sich das Instanzverzeichnis im Ausgangsverzeichnis der Benutzer-ID tsminst1: /home/tsminst1/tsminst1

Sie können das Verzeichnis auch an einer anderen Position erstellen, zum Beispiel: /tsmserver/tsminst1

Im Instanzverzeichnis sind folgende Dateien für die Serverinstanz gespeichert:

- Serveroptionsdatei dsmserv.opt
- Die Serverschlüsseldatenbankdatei cert.kdb und die .arm-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
- Einheitenkonfigurationsdatei, wenn die Serveroption DEVCONFIG keinen vollständig qualifizierten Namen angibt
- Protokolldatei für Datenträger, wenn die Serveroption VOLUMEHISTORY keinen vollständig qualifizierten Namen angibt
- Datenträger für Speicherpools mit dem Typ **DEVTYPE**=**FILE**, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
- Benutzerexits
- Traceausgabe (wenn nicht vollständig qualifiziert)

Datenbankname

Der Datenbankname lautet für jede Serverinstanz immer TSMDB1. Dieser Name kann nicht geändert werden.

Servername

Der Servername ist ein interner Name für IBM Spectrum Protect und wird für Operationen verwendet, bei denen eine Datenübertragung zwischen mehreren IBM Spectrum Protect-Servern auftritt. Zum Beispiel bei der Kommunikation zwischen Servern und bei der gemeinsamen Nutzung von Speicherarchiven.

Der Servername wird auch verwendet, wenn Sie den Server dem Operations Center hinzufügen, so dass er mit dieser Schnittstelle verwaltet werden kann. Verwenden Sie einen eindeutigen Namen für jeden Server. Verwenden Sie einen Namen, der die Position oder den Zweck des Servers angibt, um die Identifikation im Operations Center (oder mit einem Befehl **QUERY SERVER**) zu erleichtern. Nachdem ein IBM Spectrum Protect-Server als Hub- oder Peripherieserver konfiguriert wurde, dürfen Sie seinen Namen nicht mehr ändern.

Wenn Sie den Assistenten verwenden, wird als Standardname der Hostname des von Ihnen verwendeten Systems vorgeschlagen. Sie können einen anderen, für Ihre Umgebung aussagekräftigen Namen verwenden. Befinden sich mehrere Server auf dem System, können Sie bei Verwendung des Assistenten den Standardnamen nur für einen der Server angeben. Sie müssen einen eindeutigen Namen für jeden Server eingeben.

Zum Beispiel:

```
LOHNBUCHHALTUNG
VERTRIEB
```

Verzeichnisse für Datenbankbereich und Wiederherstellungsprotokoll

Die Verzeichnisse können gemäß den lokalen Vorgaben benannt werden. Sie sollten Namen verwenden, die die Verzeichnisse mit der Serverinstanz verknüpfen, um die Identifikation zu erleichtern.

Beispiel für das Archivprotokoll:

```
/tsminst1_archlog
```

Installationsverzeichnisse

Zu den Installationsverzeichnissen für den IBM Spectrum Protect-Server gehören die Verzeichnisse für den Server, IBM Db2, die Einheiten, die Sprache und andere Verzeichnisse. Jedes Verzeichnis enthält mehrere zusätzliche Verzeichnisse.

Das Verzeichnis `/opt/tivoli/tsm/server/bin` ist das Standardverzeichnis, das den Servercode und die Lizenzierung enthält.

Das während der Installation des IBM Spectrum Protect-Servers installierte Db2-Produkt hat die in den Db2-Informationsquellen dokumentierte Verzeichnisstruktur. Schützen Sie diese Verzeichnisse und Dateien wie die Serververzeichnisse. Das Standardverzeichnis heißt `/opt/tivoli/tsm/db2`.

Sie können folgende Sprachen verwenden: Englisch (US), Deutsch, Französisch, Italienisch, Spanisch, Portugiesisch (Brasilien), Koreanisch, Japanisch, traditionelles Chinesisch, vereinfachtes Chinesisch, Chinesisch GBK, Chinesisch Big5 und Russisch.

Kapitel 2. Serverkomponenten installieren

Für die Installation der IBM Spectrum Protect-Serverkomponenten können Sie den Installationsassistenten oder die Befehlszeile im Konsolenmodus verwenden.

Informationen zu diesem Vorgang

Mithilfe der IBM Spectrum Protect-Installationssoftware können Sie die folgenden Komponenten installieren:

- Server

  Tipp: Die Datenbank (IBM Db2), Global Security Kit (GSKit) und IBM Java Runtime Environment (JRE) werden automatisch installiert, wenn Sie die Serverkomponente auswählen.
- Sprachen des Servers
- Lizenz
- Einheiten
- IBM Spectrum Protect for SAN
- Operations Center

Für die Installation eines Servers anhand dieses Leitfadens müssen Sie 30 - 45 Minuten einplanen.

Installationspaket abrufen

Das Installationspaket für IBM Spectrum Protect kann von einer IBM Download-Site heruntergeladen werden, z. B. von Passport Advantage oder IBM Fix Central.

Vorbereitende Schritte

Wenn Sie die Dateien herunterladen wollen, legen Sie als Systembenutzergrenzwert für die maximale Dateigröße 'unlimited' (unbegrenzt) fest, um sicherzustellen, dass die Dateien ordnungsgemäß heruntergeladen werden können:

1. Geben Sie den folgenden Befehl aus, um den Wert für die maximale Dateigröße abzufragen:

   ```
   ulimit -Hf
   ```
2. Wenn als Systembenutzergrenzwert für die maximale Dateigröße nicht 'unlimited' (unbegrenzt) angegeben ist, geben Sie 'unlimited' gemäß den Anweisungen in der Dokumentation Ihres Betriebssystems an.

Vorgehensweise

1. Laden Sie die entsprechende Paketdatei von einer der folgenden Websites herunter:
   - Laden Sie das Serverpaket aus Passport Advantage oder Fix Central herunter.
   - Die neuesten Informationen, Aktualisierungen und Fixes finden Sie im IBM Support Portal.
2. Gehen Sie wie folgt vor, wenn Sie das Paket von einer IBM Download-Site heruntergeladen haben:
   a. Überprüfen Sie, ob genug Speicherbereich zum Speichern der Installationsdateien nach dem Extrahieren aus dem Produktpaket vorhanden ist. Informationen zum Speicherplatzbedarf finden Sie im Downloaddokument:
      - IBM Spectrum Protect Technote 588021
      - IBM Spectrum Protect Extended Edition Technote 588023
      - IBM Spectrum Protect for Data Retention Technote 588025

b. Laden Sie die Paketdatei in ein beliebiges Verzeichnis herunter. Der Pfad darf maximal 128 Zeichen enthalten. Sie müssen die Installationsdateien in ein leeres Verzeichnis extrahieren. Verwenden Sie kein Verzeichnis, das bereits extrahierte Dateien oder andere Dateien enthält.

c. Stellen Sie sicher, dass die Berechtigung zur Ausführung für das Paket definiert ist. Bei Bedarf können Sie die Dateiberechtigungen mit dem folgenden Befehl ändern:

```
chmod a+x Paketname.bin
```

d. Geben Sie den folgenden Befehl aus, um das Paket zu extrahieren:

```
./Paketname.bin
```

Paketname ist der Name der heruntergeladenen Datei. Zum Beispiel:

```
8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
8.1.x.000-IBM-SPSRV-Linuxs390x.bin
8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
```

3. Wählen Sie eine der folgenden Methoden für die Installation von IBM Spectrum Protect aus:
   - „IBM Spectrum Protect mit dem Installationsassistenten installieren” auf Seite 84
   - „IBM Spectrum Protect im Konsolenmodus installieren” auf Seite 85
   - „IBM Spectrum Protect im unbeaufsichtigten Modus installieren” auf Seite 85
4. Nachdem Sie IBM Spectrum Protect installiert haben und bevor Sie das Produkt für Ihre Verwendung anpassen, rufen Sie das

   IBM Support Portal auf. Klicken Sie auf **Support and downloads** und legen Sie alle gültigen Fixes an.

IBM Spectrum Protect mit dem Installationsassistenten installieren

Sie können den Server mit dem grafisch orientierten Assistenten von IBM Installation Manager installieren.

Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:

- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.

Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

Option	Bezeichnung
Installation der Software mithilfe eines heruntergeladenen Pakets:	a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben. b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten zu starten: `./install.sh`

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM Installation Manager-Verzeichnis `logs` gespeichert werden.

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

- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf **Downloads (fixes and PTFs)** und legen Sie alle gültigen Fixes an.
- Nachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Kapitel 3, „Die ersten Schritte nach der Installation von IBM Spectrum Protect", auf Seite 89, um zu erfahren, wie Ihr Server konfiguriert wird.

IBM Spectrum Protect im Konsolenmodus installieren

Sie können IBM Spectrum Protect mithilfe der Befehlszeile im Konsolenmodus installieren.

Vorbereitende Schritte

Führen Sie vor dem Start der Installation die folgenden Schritte aus:

- Überprüfen Sie, ob für das Betriebssystem die erforderliche Sprache definiert ist. Die Sprache des Betriebssystems ist standardmäßig die Sprache des Installationsassistenten.

Vorgehensweise

Installieren Sie IBM Spectrum Protect mit dem folgenden Verfahren:

Option	Bezeichnung
Installation der Software mithilfe eines heruntergeladenen Pakets:	a. Wechseln Sie in das Verzeichnis, in das Sie das Paket heruntergeladen haben. b. Geben Sie den folgenden Befehl aus, um den Installationsassistenten im Konsolenmodus zu starten: `./install.sh -c` **Optional :** Generieren Sie während einer Installation im Konsolenmodus eine Antwortdatei. Geben Sie die Optionen für die Installation im Konsolenmodus und in der Anzeige **Zusammenfassung** G an, um die Antworten zu generieren.

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM Installation Manager-Verzeichnis `logs` gespeichert werden. Zum Beispiel:

  ```
  /var/ibm/InstallationManager/logs
  ```

- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf **Downloads (fixes and PTFs)** und legen Sie alle gültigen Fixes an.
- Nachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Kapitel 3, „Die ersten Schritte nach der Installation von IBM Spectrum Protect", auf Seite 89, um zu erfahren, wie Ihr Server konfiguriert wird.

IBM Spectrum Protect im unbeaufsichtigten Modus installieren

Sie können den Server im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.

Vorbereitende Schritte

Für die Dateneingabe bei Verwendung der unbeaufsichtigten Installation können Sie eine Antwortdatei verwenden. Die folgenden Musterantwortdateien stehen im Verzeichnis `input` zur Verfügung, in dem das Installationspaket extrahiert wird:

`install_response_sample.xml`
Verwenden Sie diese Datei für die Installation der IBM Spectrum Protect-Komponenten.

`update_response_sample.xml`
Verwenden Sie diese Datei für das Upgrade der IBM Spectrum Protect-Komponenten.

Diese Dateien enthalten Standardwerte, die dazu beitragen können, unnötige Warnungen zu vermeiden. Befolgen Sie die in den Dateien enthaltenen Anweisungen zur Verwendung dieser Dateien.

Wenn Sie eine Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

Vorgehensweise

1. Erstellen Sie eine Antwortdatei.

   Sie können die Musterantwortdatei ändern oder eine eigene Datei erstellen.
2. Wenn Sie den Server und das Operations Center im unbeaufsichtigten Modus installieren, erstellen Sie in der Antwortdatei ein Kennwort für den Truststore des Operations Center.

   Wenn Sie die Datei `install_response_sample.xml` verwenden, fügen Sie das Kennwort in die folgende Zeile der Datei ein. Hierbei ist *`mein_Kennwort`* das Kennwort:

   ```
   <variable name='ssl.password' value='mein_Kennwort'/>
   ```

   Weitere Informationen zu diesem Kennwort finden Sie in Prüfliste für die Installation.

   Tipp: Das Truststore-Kennwort ist nicht erforderlich, wenn Sie das Operations Center mit der Datei `update_response_sample.xml` aktualisieren.
3. Geben Sie den folgenden Befehl in dem Verzeichnis, in dem das Installationspaket extrahiert wurde, aus, um die unbeaufsichtigte Installation zu starten. Der Wert *Antwortdatei* gibt den Pfad und den Namen der Antwortdatei an.

   - ```
     ./install.sh -s -input Antwortdatei -acceptLicense
     ```

Nächste Schritte

- Wenn während des Installationsprozesses Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM Installation Manager-Verzeichnis `logs` gespeichert werden. Zum Beispiel:

  ```
  /var/ibm/InstallationManager/logs
  ```
- Nachdem Sie den Server und die Komponenten installiert haben und bevor Sie sie für Ihre Verwendung anpassen, rufen Sie das IBM Support Portal auf. Klicken Sie auf **Downloads (fixes and PTFs)** und legen Sie alle gültigen Fixes an.
- Nachdem Sie einen neuen Server installiert haben, lesen Sie den Abschnitt Kapitel 3, „Die ersten Schritte nach der Installation von IBM Spectrum Protect”, auf Seite 89, um zu erfahren, wie Ihr Server konfiguriert wird.

Serversprachenpakete installieren

Übersetzungen für den Server ermöglichen das Anzeigen von Nachrichten und Hilfetext auf dem Server in verschiedenen Sprachen. Die Übersetzungen gestatten auch die Verwendung länderspezifischer Einstellungen für das Datums-, Uhrzeit- und Zahlenformat.
  ```

Vorbereitende Schritte

Anweisungen zur Installation von von Sprachenpaketen für Speicheragenten finden Sie unter Language pack configuration for Storage Agent.

Spracheinstellungen für den Server

Verwenden Sie zum Anzeigen von Servernachrichten und Hilfetext entweder das Standardsprachenpaket oder wählen Sie ein anderes Sprachenpaket aus.

Dieses Sprachenpaket wird automatisch für die folgende Standardsprachenoption für IBM Spectrum Protect-Servernachrichten und -Hilfetext installiert:

- LANGUAGE en_US

Für vom Standard abweichende Sprachen oder Ländereinstellungen installieren Sie das für Ihre Installation erforderliche Sprachenpaket.

Sie können die aufgeführten Sprachen verwenden:

Tabelle 19. Serversprachen für Linux

Sprache	**Wert der Option LANGUAGE**
Chinesisch, vereinfacht	zh_CN
	zh_CN.gb18030
	zh_CN.utf8
Chinesisch, traditionell	Big5 / Zh_TW
	zh_TW
	zh_TW.utf8
Englisch, Vereinigte Staaten	en_US
	en_US.utf8
Französisch	fr_FR
	fr_FR.utf8
Deutsch	de_DE
	de_DE.utf8
Italienisch	it_IT
	it_IT.utf8
Japanisch	ja_JP
	ja_JP.utf8
Koreanisch	ko_KR
	ko_KR.utf8
Portugiesisch, Brasilianisches	pt_BR
	pt_BR.utf8
Russisch	ru_RU
	ru_RU.utf8

Tabelle 19. Serversprachen für Linux (Forts.)	
Sprache	**Wert der Option LANGUAGE**
Spanisch	es_ES
	es_ES.utf8

Einschränkung: Bei Verwendung des Operations Center werden einige Zeichen möglicherweise nicht ordnungsgemäß angezeigt, wenn der Web-Browsers und der Server nicht dieselbe Sprache verwenden. Wenn dieses Problem auftritt, geben Sie im Browser dieselbe Sprache wie im Server an.

Sprachenpaket konfigurieren

Nach der Konfiguration eines Sprachenpakets werden Nachrichten und Hilfetext auf dem Server in der Sprache dieses Sprachenpakets und nicht in Englisch (US) angezeigt. Installationspakete werden mit IBM Spectrum Protect zur Verfügung gestellt.

Informationen zu diesem Vorgang

Führen Sie eine der folgenden Tasks aus, um die Unterstützung für eine bestimmte Ländereinstellung zu aktivieren:

- Geben Sie in der Option LANGUAGE in der Serveroptionsdatei den Namen der Ländereinstellung an, die verwendet werden soll. Beispiel:

  Soll die Ländereinstellung `it_IT` verwendet werden, setzen Sie die Option LANGUAGE auf `it_IT`. Siehe „Spracheinstellungen für den Server” auf Seite 87.
- Wenn Sie den Server im Vordergrund starten, definieren Sie die Umgebungsvariable LC_ALL gemäß dem in der Serveroptionsdatei definierten Wert. Soll beispielsweise die Umgebungsvariable für Italienisch definiert werden, geben Sie folgenden Wert ein:

```
export LC_ALL=it_IT
```

Wenn die Ländereinstellung erfolgreich initialisiert wird, steuert sie die Datums-, Uhrzeit- und Zahlenformatierung für den Server. Wenn die Ländereinstellung nicht erfolgreich initialisiert wird, verwendet der Server die englischen (US) Nachrichtendateien und das Datums-, Uhrzeit- und Zahlenformat der englischen (US) Ländereinstellung.

Sprachenpaket aktualisieren

Sie können ein Sprachenpaket mithilfe von IBM Installation Manager ändern oder aktualisieren.

Informationen zu diesem Vorgang

Sie können ein anderes Sprachenpaket in derselben IBM Spectrum Protect-Instanz installieren.

- Verwenden Sie die Funktion **Ändern** von IBM Installation Manager, um ein anderes Sprachenpaket zu installieren.
- Verwenden Sie die Funktion **Aktualisieren** von IBM Installation Manager, um eine Aktualisierung auf neuere Versionen der Sprachenpakete durchzuführen.

Tipp: In IBM Installation Manager bedeutet *aktualisieren* das Erkennen und Installieren von Aktualisierungen und Fixes für installierte Softwarepakete. In diesem Kontext sind *Aktualisierung* und *Upgrade* gleichbedeutend.

Kapitel 3. Die ersten Schritte nach der Installation von IBM Spectrum Protect

Nach der Installation von IBM Spectrum Protect bereiten Sie die Konfiguration vor. Bevorzugte Methode für die Konfiguration der IBM Spectrum Protect-Instanz ist die Verwendung des Konfigurationsassistenten.

Informationen zu diesem Vorgang

1. Aktualisieren Sie die Kernelparameterwerte. Siehe Kernelparameter für Linux-Systeme optimieren.
2. Erstellen Sie die Verzeichnisse und die Benutzer-ID für die Serverinstanz. Siehe „Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen” auf Seite 91.
3. Konfigurieren Sie eine Serverinstanz. Wählen Sie eine der folgenden Optionen aus:
   - Verwenden Sie den Konfigurationsassistenten (die bevorzugte Methode). Siehe „IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren” auf Seite 93.
   - Konfigurieren Sie die neue Instanz manuell. Siehe „Serverinstanz manuell konfigurieren” auf Seite 93. Führen Sie während einer manuellen Konfiguration die folgenden Schritte aus:
     a. Definieren Sie Ihre Verzeichnisse und erstellen Sie die IBM Spectrum Protect-Instanz. Siehe „Serverinstanz erstellen” auf Seite 93.
     b. Erstellen Sie eine neue Serveroptionsdatei, indem Sie die Musterdatei kopieren, um die Datenübertragung zwischen dem Server und den Clients zu definieren. Siehe „Server- und Clientübertragung konfigurieren” auf Seite 95.
     c. Geben Sie den Befehl **DSMSERV FORMAT** aus, um die Datenbank zu formatieren. Siehe „Datenbank und Protokoll formatieren” auf Seite 98.
     d. Konfigurieren Sie Ihr System für die Datenbanksicherung. Siehe „Datenbankmanager für die Datenbanksicherung vorbereiten” auf Seite 99.
4. Konfigurieren Sie Optionen, die die Ausführung der Datenbankreorganisation steuern. Siehe „Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren” auf Seite 101.
5. Starten Sie die Serverinstanz, falls noch nicht gestartet.

   Siehe „Serverinstanz starten” auf Seite 102.
6. Registrieren Sie Ihre Lizenz. Siehe „Lizenzregistrierung” auf Seite 108.
7. Bereiten Sie Ihr System auf Datenbanksicherungen vor. Siehe „Server für Datenbanksicherungsoperationen vorbereiten” auf Seite 108.
8. Um die Fehlerbehebung für den Fall späterer Probleme zu erleichtern, stellen Sie sicher, dass genügend Speicherbereich für einen Kernspeicherauszug zugeordnet ist. Weitere Informationen finden Sie in Technote 6357399.
9. Überwachen Sie den Server. Siehe „Server überwachen” auf Seite 110.

Kernelparameter optimieren

Damit IBM Spectrum Protect und IBM Db2 unter Linux ordnungsgemäß installiert und ausgeführt werden, müssen Sie die Kernelkonfigurationsparameter aktualisieren.

Informationen zu diesem Vorgang

Wenn Sie diese Parameter nicht aktualisieren, kann die Installation von Db2 und IBM Spectrum Protect fehlschlagen. Auch wenn die Installation erfolgreich verläuft, können Betriebsfehler auftreten, wenn Sie keine Parameterwerte definieren.

Kernelparameter aktualisieren

IBM Db2 erhöht IPC-Kernelparameterwerte automatisch auf die bevorzugten Einstellungen (IPC = Interprocess Communication, Interprozesskommunikation).

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um die Kernelparameter auf Linux-Servern zu aktualisieren:

Vorgehensweise

1. Geben Sie den Befehl **`ipcs -l`** aus, um die Parameterwerte aufzulisten.
2. Analysieren Sie die Ergebnisse, um festzustellen, ob für Ihr System Änderungen erforderlich sind.
   Wenn Änderungen erforderlich sind, können Sie den Parameter in der Datei `/etc/sysctl.conf` definieren. Der Parameterwert wird beim Systemstart angewendet.

Nächste Schritte

In Red Hat Enterprise Linux 6 (RHEL6) müssen Sie den Parameter `kernel.shmmax` in der Datei `/etc/sysctl.conf` definieren, bevor der IBM Spectrum Protect-Server beim Systemstart automatisch gestartet wird.

Ausführliche Informationen zur Db2-Datenbank für Linux finden Sie in der Db2-Produktinformation.

Vorgeschlagene Einstellungen

Stellen Sie sicher, dass die Werte für Kernelparameter ausreichen, um Betriebsfehler während der Ausführung des IBM Spectrum Protect-Servers zu verhindern.

Informationen zu diesem Vorgang

Die folgende Tabelle enthält Beschreibungen der Kernelparameter für die Ausführung von IBM Spectrum Protect und IBM Db2.

Optimale Einstellungen für Kernelparameter	
Parameter	**Beschreibung**
kernel.randomize_va_space	Der Parameter **`kernel.randomize_va_space`** konfiguriert die Verwendung von Speicher-ASLR für den Kernel. Inaktivieren Sie ASLR, da ASLR Fehler für die Db2-Software verursachen kann. Ausführliche Informationen zu Linux ASLR und Db2 finden Sie in der Technote unter http://www.ibm.com/support/docview.wss?uid=swg21365583.
vm.swappiness	Der Parameter **`vm.swappiness`** legt fest, ob der Kernel Anwendungsspeicher aus dem physischen Arbeitsspeicher (RAM) auslagern kann. Weitere Informationen zu Kernelparametern finden Sie unter Db2-Produktinformation.
vm.overcommit_memory	Der Parameter **`vm.overcommit_memory`** hat Einfluss auf die Größe des virtuellen Speichers, deren Zuordnung der Kernel zulassen kann. Weitere Informationen zu Kernelparametern finden Sie unter Db2-Produktinformation.

Benutzer-ID und Verzeichnisse für die Serverinstanz erstellen

Erstellen Sie die Benutzer-ID für die IBM Spectrum Protect-Serverinstanz und die Verzeichnisse, die die Serverinstanz für Datenbank- und Wiederherstellungsprotokolle benötigt.

Vorbereitende Schritte

Lesen Sie die Informationen zur Planung des Speicherbereichs für den Server, bevor Sie diese Task ausführen. Siehe „Arbeitsblätter für Planungsdetails für den Server” auf Seite 60.

Vorgehensweise

1. Erstellen Sie die Benutzer-ID, die Eigner der Serverinstanz sein soll.

   Diese Benutzer-ID verwenden Sie später bei der Erstellung der Serverinstanz.

   Erstellen Sie eine Benutzer-ID und eine Gruppe, die Eigner der Serverinstanz sein sollen.

   a. Die folgenden Befehle können mit einer Verwaltungsbenutzer-ID ausgeführt werden, die den Benutzer und die Gruppe definieren soll. Erstellen Sie die Benutzer-ID und Gruppe im Ausgangsverzeichnis des Benutzers.

      Einschränkung: In der Benutzer-ID dürfen nur Kleinbuchstaben (a-z), Ziffern (0-9) und das Unterstreichungszeichen (_) verwendet werden. Die Benutzer-ID und der Gruppenname müssen die folgenden Regeln einhalten:

      - Die maximale Länge beträgt 8 Zeichen.
      - Die Benutzer-ID und der Gruppenname dürfen nicht mit *ibm*, *sql*, *sys* oder mit einer Ziffer beginnen.
      - Als Benutzer-ID und Gruppenname dürfen nicht *user*, *admin*, *guest*, *public*, *local* und kein reserviertes SQL-Wort verwendet werden.

      Erstellen Sie beispielsweise die Benutzer-ID `tsminst1` in der Gruppe `tsmsrvrs`. Die folgenden Beispiele zeigen, wie diese Benutzer-ID und diese Gruppe mit Betriebssystembefehlen erstellt werden.

      ```
      groupadd tsmsrvrs -g 1111
      useradd -d /home/tsminst1 -u 2222 -g 1111 -s /bin/bash tsminst1
      passwd tsminst1
      ```

      Einschränkung: IBM Db2 unterstützt nicht die direkte Authentifizierung von Betriebssystembenutzern durch LDAP.

   b. Melden Sie sich ab und dann bei Ihrem System an. Wechseln Sie zu dem gerade erstellten Benutzerkonto. Verwenden Sie ein interaktives Anmeldeprogramm, z. B. Telnet, damit Sie zur Eingabe des Kennworts aufgefordert werden und es ggf. ändern können.

2. Erstellen Sie die vom Server benötigten Verzeichnisse.

Erstellen Sie leere Verzeichnisse für jeden Tabelleneintrag und stellen Sie sicher, dass die neue Benutzer-ID, die Sie gerade erstellt haben, Eigner der Verzeichnisse ist. Hängen Sie den zugeordneten Speicher in jedem der Verzeichnisse für aktive Protokolldateien, für Archivprotokolle und Datenbanken an.		
Element	**Beispielbefehle für die Verzeichniserstellung**	**Ihre Verzeichnisse**
Das *Instanzverzeichnis* für den Server. Dieses Verzeichnis enthält spezielle Dateien für diese Serverinstanz (die Serveroptionsdatei und andere serverspezifische Dateien).	`mkdir /tsminst1`	

Die Datenbankverzeichnisse	`mkdir /tsmdb001`
	`mkdir /tsmdb002`
	`mkdir /tsmdb003`
	`mkdir /tsmdb004`	

Verzeichnis für aktive Protokolldateien	`mkdir /tsmlog`	
Verzeichnis für Archivprotokolle	`mkdir /tsmarchlog`	
Optional: Verzeichnis für den Protokollspiegel für die aktive Protokolldatei	`mkdir /tsmlogmirror`	
Optional: Sekundäres Verzeichnis für Archivprotokolle (Übernahmeverzeichnis für Archivprotokolle)	`mkdir /tsmarchlogfailover`	

Wenn ein Server anfänglich mit dem Dienstprogramm **DSMSERV FORMAT** oder mit dem Konfigurationsassistenten erstellt wird, werden eine Serverdatenbank und ein Wiederherstellungsprotokoll erstellt. Außerdem werden Dateien zum Speichern von Datenbankinformationen erstellt, die vom Datenbankmanager verwendet werden.

3. Melden Sie die neue Benutzer-ID ab.

IBM Spectrum Protect-Server konfigurieren

Nachdem Sie den Server installiert und für die Konfiguration vorbereitet haben, konfigurieren Sie die Serverinstanz.

Informationen zu diesem Vorgang

Wählen Sie eine der folgenden Optionen aus, um eine IBM Spectrum Protect-Serverinstanz zu konfigurieren:

- Verwenden Sie den IBM Spectrum Protect-Konfigurationsassistenten auf Ihrem lokalen System. Siehe „IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren” auf Seite 93.
- Konfigurieren Sie die neue IBM Spectrum Protect-Instanz manuell. Siehe „Serverinstanz manuell konfigurieren” auf Seite 93. Führen Sie während einer manuellen Konfiguration die folgenden Schritte aus:
  1. Definieren Sie die Verzeichnisse und erstellen Sie die IBM Spectrum Protect-Instanz. Siehe „Serverinstanz erstellen” auf Seite 93.

2. Erstellen Sie eine neue Serveroptionsdatei, indem Sie die Musterdatei kopieren, um die Datenübertragung zwischen dem IBM Spectrum Protect-Server und den Clients zu definieren. Siehe „Server- und Clientübertragung konfigurieren" auf Seite 95 .
3. Geben Sie den Befehl DSMSERV FORMAT aus, um die Datenbank zu formatieren. Siehe „Datenbank und Protokoll formatieren" auf Seite 98.
4. Konfigurieren Sie Ihr System für die Datenbanksicherung. Siehe „Datenbankmanager für die Datenbanksicherung vorbereiten" auf Seite 99.

IBM Spectrum Protect mit dem Konfigurationsassistenten konfigurieren

Der Assistent stellt eine Möglichkeit zur Konfiguration eines Servers mit Anleitung dar. Wenn Sie die grafische Benutzerschnittstelle (GUI) verwenden, können Sie einige komplexe Konfigurationsschritte der manuellen Ausführung vermeiden. Starten Sie den Assistenten auf dem System, auf dem Sie das IBM Spectrum Protect-Serverprogramm installiert haben.

Vorbereitende Schritte

Bevor Sie den Konfigurationsassistenten verwenden, müssen Sie alle vorhergehenden Schritte zur Vorbereitung der Konfiguration ausführen. Zu diesen Schritten gehören die Installation von IBM Spectrum Protect, die Erstellung der Datenbank- und Protokollverzeichnisse und die Erstellung der Verzeichnisse und der Benutzer-ID für die Serverinstanz.

Vorgehensweise

1. Stellen Sie sicher, dass folgende Anforderungen erfüllt sind:
   - Das System, auf dem Sie IBM Spectrum Protect installiert haben, muss über den X Window System-Client verfügen. Außerdem müssen Sie einen X Window System-Server auf Ihrem Desktop ausführen.
   - Im System muss das SSH-Protokoll (Secure Shell) aktiviert sein. Stellen Sie sicher, dass für den Port der Standardwert 22 definiert ist und dass der Port nicht durch eine Firewall blockiert wird. Sie müssen die Kennwortauthentifizierung in der Datei `sshd_config` im Verzeichnis `/etc/ssh/` aktivieren. Stellen Sie außerdem sicher, dass der SSH-Dämonservice über Zugriffsberechtigungen zum Herstellen einer Verbindung zum System mithilfe des Werts `localhost` verfügt.
   - Sie müssen sich mit der Benutzer-ID, die Sie für die Serverinstanz erstellt haben, mit dem SSH-Protokoll beim System anmelden können. Bei Verwendung des Assistenten müssen Sie diese Benutzer-ID und dieses Kennwort für den Zugriff auf dieses System angeben.
2. Starten Sie die lokale Version des Assistenten:

   Öffnen Sie das Programm `dsmicfgx` im Verzeichnis `/opt/tivoli/tsm/server/bin`. Dieser Assistent kann nur mit der Rootbenutzer-ID ausgeführt werden.

   Befolgen Sie die Anweisungen zur Ausführung der Konfiguration. Der Assistent kann gestoppt und erneut gestartet werden. Der Server ist jedoch erst betriebsbereit, wenn der gesamte Konfigurationsprozess abgeschlossen ist.

Serverinstanz manuell konfigurieren

Nach der Installation von IBM Spectrum Protect können Sie IBM Spectrum Protect auch manuell und nicht mit dem Konfigurationsassistenten konfigurieren.

Serverinstanz erstellen

Erstellen Sie eine IBM Spectrum Protect-Instanz mit dem Befehl **`db2icrt`**.

Informationen zu diesem Vorgang

Auf einer Workstation kann mindestens eine Serverinstanz vorhanden sein.

Wichtig: Stellen Sie Folgendes sicher, bevor der Befehl **db2icrt** ausgeführt wird:

- Das Ausgangsverzeichnis für den Benutzer (`/home/tsminst1`) ist vorhanden. Ist kein Ausgangsverzeichnis vorhanden, müssen Sie es erstellen.

  Im Instanzverzeichnis sind folgende Dateien gespeichert, die vom IBM Spectrum Protect-Server generiert werden:

  – Serveroptionsdatei `dsmserv.opt`
  – Die Serverschlüsseldatenbankdatei `cert.kdb` und die `.arm`-Dateien (werden von Clients und anderen Servern zum Importieren der Secure Sockets Layer-Zertifikate des Servers verwendet)
  – Einheitenkonfigurationsdatei, wenn die Serveroption `DEVCONFIG` keinen vollständig qualifizierten Namen angibt
  – Protokolldatei für Datenträger, wenn die Serveroption `VOLUMEHISTORY` keinen vollständig qualifizierten Namen angibt
  – Datenträger für Speicherpools mit dem Typ **DEVTYPE**=**FILE**, wenn das Verzeichnis für die Einheitenklasse nicht vollständig angegeben oder nicht vollständig qualifiziert ist
  – Benutzerexits
  – Traceausgabe (wenn nicht vollständig qualifiziert)
- Eine Sicherungskopie der folgenden Dateien muss an einer sicheren Position gespeichert werden:
  – Masterverschlüsselungsschlüsseldateien (`dsmkeydb.*`)
  – Dateien mit Serverzertifikaten und privaten Schlüsseln (`cert.*`)
- The root user and instance-user ID must have write permission to the shell configuration file. Eine Shellkonfigurationsdatei (z. B. `.profile`) ist im Ausgangsverzeichnis vorhanden. Weitere Informationen finden Sie in Db2-Produktinformation. Suchen Sie dort nach den Einstellungen für Linux- und UNIX-Umgebungsvariablen.

1. Melden Sie sich mit der Root-ID an und erstellen Sie eine IBM Spectrum Protect-Instanz. Der Name der Instanz muss mit dem Namen des Benutzers identisch sein, der Eigner der Instanz ist. Verwenden Sie den Befehl **db2icrt** und geben Sie den Befehl in eine Zeile ein:

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   Instanzname Instanzname
   ```

   Lautet Ihre Benutzer-ID für diese Instanz z. B. tsminst1, verwenden Sie den folgenden Befehl, um die Instanz zu erstellen. Geben Sie den Befehl in eine einzelne Zeile ein.

   ```
   /opt/tivoli/tsm/db2/instance/db2icrt -a server -u
   tsminst1 tsminst1
   ```

   Hinweis: Verwenden Sie ab diesem Punkt diese neue Benutzer-ID für die Konfiguration Ihres IBM Spectrum Protect-Servers. Melden Sie sich mit der Root-ID ab und mit der neuen Instanzbenutzer-ID an.
2. Geben Sie als Standardverzeichnis für die Datenbank das Instanzverzeichnis für den Server an. Sind mehrere Server vorhanden, melden Sie sich mit der Instanz-ID des jeweiligen Servers an. Geben Sie den folgenden Befehl aus:

   ```
   db2 update dbm cfg using dftdbpath Instanzverzeichnis
   ```

   Lautet das Instanzverzeichnis für den Server z. B. 'tsminst1', ändern Sie mit dem folgenden Befehl das Standardverzeichnis für die Datenbank in 'tsminst1':

   ```
   db2 update dbm cfg using dftdbpath /tsminst1
   ```
3. Ändern Sie den Bibliothekspfad so, dass Bibliotheken eingeschlossen werden, die für Serveroperationen erforderlich sind.

   Tipp: In den folgenden Beispielen sind die Verzeichnisse aufgeführt:

- *Verzeichnis_server_bin* ist ein Unterverzeichnis des Serverinstallationsverzeichnisses. Zum Beispiel `/opt/tivoli/tsm/server/bin`.
- *Instanzbenutzer-Ausgangsverzeichnis* ist das Ausgangsverzeichnis des Instanzbenutzers. Zum Beispiel `/home/tsminst1`.

.

- Sie müssen eine der folgenden Dateien aktualisieren, um den Bibliothekspfad zu definieren, wenn IBM Db2 oder der Server gestartet wird. Führen Sie die Aktualisierung auf der Basis der Shell aus, für deren Verwendung der Instanzbenutzer konfiguriert ist.

  Bash- oder Korn-Shell:

  ```
  Instanzbenutzer-Ausgangsverzeichnis/sqllib/userprofile
  ```

  C-Shell:

  ```
  Instanzbenutzer-Ausgangsverzeichnis/sqllib/usercshrc
  ```

- Führen Sie die Aktualisierung auf der Basis der Shell aus, für deren Verwendung der Instanzbenutzer konfiguriert ist.

  Bash- oder Korn-Shell:

  Fügen Sie den folgenden Eintrag zur Datei *Instanzbenutzer-Ausgangsverzeichnis*`/sqllib/userprofile` in einer einzigen Zeile hinzu:

  ```
  export LD_LIBRARY_PATH=server_bin_directory/
  dbbkapi:/usr/local/ibm/gsk8_64/lib64:
  /opt/ibm/lib:
  /opt/ibm/lib64:$LD_LIBRARY_PATH
  ```

  C-Shell:

  Fügen Sie den folgenden Eintrag zur Datei *Instanzbenutzer-Ausgangsverzeichnis*`/sqllib/usercshrc` in einer einzigen Zeile hinzu:

  ```
  setenv LD_LIBRARY_PATH server_bin_directory/dbbkapi:/
  usr/local/ibm/gsk8_64/lib64:/
  opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH
  ```

  Hinweis: Die folgenden Einträge müssen im Bibliothekspfad enthalten sein und vor allen anderen Einträgen im Bibliothekspfad stehen:

  – `server_bin_directory/dbbkapi`
  – `/usr/local/ibm/gsk8_64/lib64`

4. Erstellen Sie eine neue Serveroptionsdatei.

Server- und Clientübertragung konfigurieren

Eine standardmäßige Beispielserveroptionsdatei mit dem Namen `dsmserv.opt.smp` wird während der IBM Spectrum Protect-Installation im Verzeichnis `/opt/tivoli/tsm/server/bin` erstellt. Sie müssen die Datenübertragung zwischen dem Server und den Clients definieren, indem Sie eine neue Serveroptionsdatei erstellen. Hierfür kopieren Sie die Musterdatei in das Verzeichnis für die Serverinstanz.

Informationen zu diesem Vorgang

Stellen Sie sicher, dass ein Serverinstanzverzeichnis, z. B. `/tsminst1`, vorhanden ist und kopieren Sie die Musterdatei in dieses Verzeichnis. Nennen Sie die neue Datei `dsmserv.opt` und editieren Sie die Optionen. Führen Sie diese Konfiguration vor der Initialisierung der Serverdatenbank aus. Jedes Beispiel bzw. jeder Standardeintrag in der Beispieloptionsdatei ist ein Kommentar in einer Zeile, die mit einem Stern (*)

beginnt. Bei Optionen muss die Groß-/Kleinschreibung nicht beachtet werden, und zwischen Schlüsselwörtern und Werten dürfen sich ein oder mehrere Leerzeichen befinden.

Für das Editieren der Optionsdatei gelten folgende Richtlinien:

- Entfernen Sie den Stern am Anfang der Zeile, um eine Option zu aktivieren.
- Beginnen Sie mit der Eingabe der Optionen in einer beliebigen Spalte.
- Geben Sie nur eine Option pro Zeile ein. Die Option muss auf einer Zeile stehen.
- Werden mehrere Einträge für ein Schlüsselwort vorgenommen, verwendet der IBM Spectrum Protect-Server den letzten Eintrag.

Wenn Sie die Serveroptionsdatei ändern, müssen Sie den Server erneut starten, damit die Änderungen wirksam werden.

Sie können mindestens eine der folgenden Übertragungsmethoden angeben:

- TCP/IP Version 4 oder Version 6
- Shared Memory
- Secure Sockets Layer (SSL)

  Tipp: Sie können Kennwörter im LDAP-Verzeichnisserver oder im IBM Spectrum Protect-Server authentifizieren. Im LDAP-Verzeichnisserver authentifizierte Kennwörter können erweiterte Systemsicherheit zur Verfügung stellen.

TCP/IP-Optionen definieren

Wählen Sie aus dem Bereich von TCP/IP-Optionen eine Option für den IBM Spectrum Protect-Server aus oder verwenden Sie den Standardwert.

Informationen zu diesem Vorgang

Das folgende Beispiel zeigt eine Liste der TCP/IP-Optionen, mit denen Sie Ihr System definieren können.

```
commmethod        tcpip
  tcpport         1500
  tcpwindowsize   0
  tcpnodelay      yes
```

Tipp: Sie können TCP/IP Version 4 und/oder Version 6 verwenden.

TCPPORT
Die Adresse des Server-Ports für TCP/IP- und SSL-Kommunikation. Der Standardwert ist 1500.

TCPWINDOWSIZE
Gibt die Größe des TCP/IP-Puffers an, der beim Senden oder Empfangen von Daten verwendet wird. Die in einer Sitzung verwendete Fenstergröße ist der kleinere Wert der Server- und Clientfenstergröße. Größere Fenstergrößen benötigen zusätzlichen Speicher, können jedoch die Leistung verbessern.

Sie können eine ganze Zahl von 0 bis 2048 angeben. Soll die Standardfenstergröße für das Betriebssystem verwendet werden, geben Sie 0 an.

TCPNODELAY
Gibt an, ob der Server kleine Nachrichten sendet oder ob TCP/IP die Nachrichten puffern soll. Das Senden kleiner Nachrichten kann den Durchsatz verbessern, erhöht jedoch die Anzahl der im Netz gesendeten Pakete. Geben Sie YES an, wenn kleine Nachrichten gesendet werden sollen, oder NO, wenn sie TCP/IP puffern soll. Der Standardwert ist YES.

TCPADMINPORT
Gibt die Anschlussnummer an, an der der TCP/IP-DFV-Treiber des Servers auf TCP/IP- oder SSL-fähige Kommunikationsanforderungen warten soll, die keine Clientsitzungen sind. Der Standardwert ist der Wert von TCPPORT.

SSLTCPPORT
(Nur SSL) Gibt die SSL-Anschlussnummer (SSL = Secure Sockets Layer) an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen des Befehlszeilenclients für Sichern/Archivieren und des Verwaltungsbefehlszeilenclients wartet.

SSLTCPADMINPORT
(Nur SSL) Gibt die Anschlussadresse an, an der der TCP/IP-DFV-Treiber des Servers auf Anforderungen für SSL-fähige Sitzungen für den Verwaltungsbefehlszeilenclient wartet.

Shared Memory-Optionen definieren

Sie können die Shared Memory-Übertragung zwischen Clients und Servern auf demselben System verwenden. Für die Verwendung von Shared Memory muss TCP/IP Version 4 auf dem System installiert sein.

Informationen zu diesem Vorgang

Das folgende Beispiel zeigt eine Einstellung für Shared Memory:

```
commmethod     sharedmem
   shmport     1510
```

In diesem Beispiel gibt **SHMPORT** die TCP/IP-Anschlussadresse eines Servers bei Verwendung von Shared Memory an. Verwenden Sie die Option **SHMPORT**, um einen anderen TCP/IP-Anschluss anzugeben. Die Standardanschlussadresse ist 1510.

COMMMETHOD kann in der IBM Spectrum Protect-Serveroptionsdatei mehrfach mit einem jeweils anderen Wert verwendet werden. Die folgende Angabe ist beispielsweise möglich:

```
commmethod tcpip
commmethod sharedmem
```

Bei Verwendung von Shared Memory empfangen Sie möglicherweise die folgende Nachricht vom Server:

```
ANR9999D shmcomm.c(1598): Thread-ID<39>
Fehler von msgget (2), Fehlernummer = 28
```

Die Nachricht bedeutet, dass eine Nachrichtenwarteschlange erstellt werden muss, der Systemgrenzwert für die maximale Anzahl Nachrichtenwarteschlangen (**MSGMNI**) jedoch überschritten würde.

Um die maximale Anzahl der Nachrichtenwarteschlangen (**MSGMNI**) auf Ihrem System zu bestimmen, geben Sie den folgenden Befehl aus:

```
cat /proc/sys/kernel/msgmni
```

Geben Sie folgenden Befehl aus, um den Wert für **MSGMNI** auf Ihrem System zu erhöhen:

```
sysctl -w kernel.msgmni=n
```

Dabei ist **n** die maximale Anzahl der Nachrichtenwarteschlangen, die auf dem System zulässig sein sollen.

Secure Sockets Layer-Optionen definieren

Mithilfe von Secure Sockets Layer (SSL) können Sie Ihre Daten und Kennwörter besser schützen.

Vorbereitende Schritte

SSL ist die Standardtechnologie für die Erstellung verschlüsselter Sitzungen zwischen Servern und Clients. SSL stellt einen sicheren Kanal für die Server- und Clientkommunikation über offene Kommunikationspfade zur Verfügung. Bei SSL wird die Identität des Servers durch Verwendung digitaler Zertifikate überprüft.

Verwenden Sie SSL für Sitzungen nur im Bedarfsfall, um eine bessere Systemleistung sicherzustellen. Sie könnten die Prozessorressourcen auf dem IBM Spectrum Protect-Server erweitern, um den erhöhten Anforderungen gerecht zu werden.

Datenbank und Protokoll formatieren

Wenn Sie den Server manuell konfigurieren, müssen Sie die Serverdatenbank und das Wiederherstellungsprotokoll formatieren. In der Datenbank werden Informationen zu Clientdaten und Serveroperationen gespeichert und das Wiederherstellungsprotokoll kann für eine Wiederherstellung nach System- und Datenträgerfehlern verwendet werden. Verwenden Sie für die Formatierung und Initialisierung der Serverdatenbank und des Wiederherstellungsprotokolls das Dienstprogramm **DSMSERV FORMAT**. Während der Initialisierung der Datenbank und des Wiederherstellungsprotokolls ist keine andere Serveraktivität zulässig.

Nach der Konfiguration der Serverübertragung können Sie die Datenbank initialisieren. Fügen Sie die Verzeichnisse nicht in Dateisysteme ein, deren Speicherplatz nicht ausreichen könnte. Wenn bestimmte Verzeichnisse (z. B. das Archivprotokoll) nicht mehr verfügbar oder voll sind, stoppt der Server. Weitere Informationen finden Sie in Kapazitätsplanung.

Exitlistenhandler definieren

Geben Sie für jede Serverinstanz ON für die Registry-Variable **DB2NOEXITLIST** an. Melden Sie sich mit der Instanzbenutzer-ID beim System an und führen Sie den folgenden Befehl aus:

```
db2set -i Name_der_Serverinstanz DB2NOEXITLIST=ON
```

Beispiel:

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```

Serverdatenbank und Wiederherstellungsprotokoll initialisieren

Verwenden Sie für die Formatierung und Initialisierung der Serverdatenbank, die eine IBM Db2-Datenbank ist, und des Wiederherstellungsprotokolls das Dienstprogramm **DSMSERV FORMAT**. Wenn das Verzeichnis der Serverinstanz z. B. */tsminst1* lautet, führen Sie die folgenden Befehle aus:

```
cd /tsminst1
dsmserv format dbdir=/tsmdb001 activelogsize=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Tipp: Wenn Sie mehrere Verzeichnisse angeben, stellen Sie sicher, dass die zu Grunde liegenden Dateisysteme dieselbe Größe haben, um einen konsistenten Grad der Parallelität für Datenbankoperationen zu gewährleisten. Wenn ein oder mehrere Verzeichnisse für die Datenbank kleiner als die anderen Verzeichnisse sind, wird dadurch das Potenzial zum optimierten parallelen Vorablesezugriff und zur Verteilung der Datenbank verringert.

Wenn die Db2-Datenbank nach der Ausführung des Befehls **DSMSERV FORMAT** nicht startet, müssen Sie möglicherweise die Mountoption NOSUID des Dateisystems inaktivieren. Sie müssen die Option unter den folgenden Umständen inaktivieren, um das System zu starten:

- Wenn die Option für das Dateisystem definiert ist, das das Verzeichnis des Db2-Instanzeigners enthält.
- Wenn die Option in einem Dateisystem definiert ist, das die Datenbank, aktive Protokolldateien, Archivprotokolle, Übernahmeprotokolle oder Spiegelprotokolle von Db2 enthält.

Nach der Inaktivierung der Option NOSUID hängen Sie das Dateisystem erneut an. Dann starten Sie die Db2-Datenbank mit dem folgenden Befehl:

```
db2start
```

Benutzer mit Verwaltungsaufgaben erstellen

Wenn die Formatierung der Datenbank und des Wiederherstellungsprotokolls beendet ist, müssen Sie einen Benutzer mit Verwaltungsaufgaben erstellen, der sich beim Server anmelden kann, und außerdem im IBM Spectrum Protect Operations Center angeben, dass eine Verbindung zum Server hergestellt werden

kann. Für die Erstellung eines Benutzers mit Verwaltungsaufgaben verwenden Sie die folgenden Befehle in einem Makro:

REGISTER ADMIN
Für den Befehl **REGISTER ADMIN** können folgende Parameter angegeben werden:

```
register admin Administrator-ID Administratorkennwort
```

Für das Kennwort gelten bestimmte Regeln in Bezug auf die Länge. Weitere Informationen finden Sie in REGISTER ADMIN (Administrator-ID registrieren).

GRANT AUTH
Für den Befehl **GRANT AUTH** können folgende Parameter angegeben werden:

```
grant auth Administrator-ID classes=Administratorklasse
```

Weitere Informationen finden Sie in GRANT AUTHORITY (Administratorberechtigung hinzufügen).

Führen Sie die folgenden Schritte aus, um einen Benutzer mit Verwaltungsaufgaben zu erstellen:

1. Erstellen Sie ein Makro, z. B. `setup.mac`.
2. Bearbeiten das Makro, so dass ein Benutzer mit Verwaltungsaufgaben registriert und diesem Benutzer Systemberechtigung erteilt wird. Geben Sie die folgenden Berechtigungsnachweise an:
   - Benutzer-ID mit Administratorberechtigung: `adminadmin`
   - Kennwort für Benutzer mit Verwaltungsaufgaben: `adminadmin1`

   ```
   register admin adminadmin adminadmin1
   grant auth adminadmin classes=system
   ```

   Sie müssen den Benutzer mit Verwaltungsaufgaben mit der Option **classes=system** erstellen, so dass der Benutzer mit Verwaltungsaufgaben andere potenzielle Benutzer mit Verwaltungsaufgaben erstellen kann, beispielsweise mit eingeschränkten Berechtigungen. Jeder dieser Benutzer mit Verwaltungsaufgaben kann dann eine Verbindung zum IBM Spectrum Protect Operations Center herstellen.
3. Soll der Benutzer mit Verwaltungsaufgaben erstellt und ihm Systemberechtigung erteilt werden, führen Sie den Befehl **DSMSERV** mit dem Parameter **runfile** und der Makrodatei aus:

   ```
   dsmserv runfile setup.mac
   ```

Der Benutzer mit Verwaltungsaufgaben kann dann die Serverinstanz starten und eine Verbindung zum Server herstellen, um andere erforderliche Schritte auszuführen (z. B. Datenbanksicherung konfigurieren).

Datenbankmanager für die Datenbanksicherung vorbereiten

Um die Daten in der Datenbank in IBM Spectrum Protect zu sichern, müssen Sie den Datenbankmanager aktivieren und die IBM Spectrum Protect-Anwendungsprogrammierschnittstelle (API) konfigurieren.

Informationen zu diesem Vorgang

Ab IBM Spectrum Protect Version 7.1 ist es nicht mehr erforderlich, das API-Kennwort während einer manuellen Konfiguration des Servers zu definieren. Wenn Sie das API-Kennwort während des manuellen Konfigurationsprozesses definieren, können Datenbanksicherungsversuche fehlschlagen.

Wenn Sie den Konfigurationsassistenten verwenden, um eine IBM Spectrum Protect-Serverinstanz zu erstellen, müssen Sie diese Schritte nicht ausführen. Wenn Sie eine Instanz manuell konfigurieren, führen Sie die folgenden Schritte aus, bevor Sie den Befehl **BACKUP DB** oder **RESTORE DB** ausgeben.

Achtung: Wenn die Datenbank nicht verwendet werden kann, ist der gesamte IBM Spectrum Protect-Server nicht verfügbar. Wenn eine Datenbank verloren geht und nicht wiederhergestellt werden kann, kann die Wiederherstellung der von diesem Server verwalteten Daten schwierig oder unmöglich sein. Daher ist es unbedingt erforderlich, die Datenbank zu sichern.

In den folgenden Befehlen müssen Sie die Beispielwerte durch Ihre tatsächlichen Werte ersetzen. In den Beispielen wird `tsminst1` für die Benutzer-ID der Serverinstanz, `/tsminst1` für das Verzeichnis der Serverinstanz und `/home/tsminst1` als Ausgangsverzeichnis der Serverinstanzbenutzer verwendet.

1. Definieren Sie die Umgebungsvariablenkonfiguration der IBM Spectrum Protect-API für die Datenbankinstanz:
   a. Melden Sie sich mit der Benutzer-ID `tsminst1` an.
   b. Wenn der Benutzer `tsminst1` angemeldet ist, stellen Sie sicher, dass die IBM Db2-Umgebung ordnungsgemäß initialisiert wird. Die Db2-Umgebung wird durch Ausführung des Scripts `/home/tsminst1/sqllib/db2profile` initialisiert, das normalerweise automatisch über das Profil der Benutzer-ID ausgeführt wird. Stellen Sie sicher, dass die `.profile`-Datei im Ausgangsverzeichnis der Instanzbenutzer vorhanden ist, z. B. `/home/tsminst1/.profile`. Wenn `.profile` das Script `db2profile` nicht ausführt, fügen Sie folgende Zeilen hinzu:

```
if [ -f /home/tsminst1/sqllib/db2profile ]; then
      . /home/tsminst1/sqllib/db2profile
  fi
```

   c. Fügen Sie in der Datei *Instanzverzeichnis*`/sqllib/userprofile` die folgenden Zeilen hinzu:

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

   Hierbei gilt Folgendes:

   - *Instanzverzeichnis* ist das Ausgangsverzeichnis des Serverinstanzbenutzers.
   - *Serverinstanzverzeichnis* ist das Serverinstanzverzeichnis.
   - *Serververzeichnis_bin* ist das Serververzeichnis 'bin'. Die Standardposition ist `/opt/tivoli/tsm/server/bin`.

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

```
setenv DSMI_CONFIG=Serverinstanzverzeichnis/tsmdbmgr.opt
setenv DSMI_DIR=Serververzeichnis_bin/dbbkapi
setenv DSMI_LOG=Serverinstanzverzeichnis
```

2. Melden Sie sich ab und als `tsminst1` erneut an oder geben Sie den folgenden Befehl aus:

```
. ~/.profile
```

   Tipp: Stellen Sie sicher, dass Sie ein Leerzeichen nach dem ersten Punkt (.) eingeben.

3. Erstellen Sie eine Datei mit dem Namen `tsmdbmgr.opt` im Verzeichnis *Serverinstanz*, das sich in diesem Beispiel im Verzeichnis `/tsminst1` befindet, und fügen Sie folgende Zeile hinzu:

```
SERVERNAME TSMDBMGR_TSMINST1
```

   Hinweis: Der Wert für SERVERNAME muss in den Dateien `tsmdbmgr.opt` und `dsm.sys` konsistent sein.

4. Fügen Sie als Rootbenutzer die folgenden Zeilen zur Konfigurationsdatei `dsm.sys` der IBM Spectrum Protect-API hinzu. Die Konfigurationsdatei `dsm.sys` befindet sich standardmäßig in folgendem Standardverzeichnis:

   Serververzeichnis_bin`/dbbkapi/dsm.sys`

```
servername TSMDBMGR_TSMINST1
commmethod tcpip
tcpserveraddr localhost
tcpport 1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

Erläuterungen:

- *Servername* stimmt mit dem Wert für `servername` in der Datei `tsmdbmgr.opt` überein.
- *commethod* gibt die Client-API an, mit der Kontakt zum Server wegen der Datenbanksicherung hergestellt wird. Gültige Werte sind `tcpip` und `sharedmem`. Weitere Informationen zu Shared Memory (gemeinsam genutzter Speicher) finden Sie in Schritt 5.
- *tcpserveraddr* gibt die Serveradresse an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Um sicherzustellen, dass die Datenbank gesichert werden kann, muss dieser Wert `localhost` lauten.

  Wichtig: Wenn auf Ihrem Server ein von einer Zertifizierungsstelle signiertes Zertifikat (CA-signiertes Zertifikat) verwendet wird, müssen Sie für die Option *tcpserveraddr* die externe IP-Adresse des Servers angeben.
- *tcpport* gibt die Anschlussnummer an, mit der die Client-API Kontakt zum Server wegen der Datenbanksicherung herstellt. Sie müssen denselben `tcpport`-Wert wie in der Serveroptionsdatei `dsmserv.opt` angeben.
- *errorlogname* gibt das Fehlerprotokoll an, in dem die Client-API Fehler protokolliert, die während einer Datenbanksicherung auftreten. Dieses Protokoll befindet sich normalerweise im Serverinstanzverzeichnis. Dieses Protokoll kann sich jedoch an jeder beliebigen Position befinden, für die die Instanzbenutzer-ID Schreibberechtigung hat.
- *nodename* gibt den Knotennamen an, mit dem die Client-API während einer Datenbanksicherung eine Verbindung zum Server herstellt. Um sicherzustellen, dass die Datenbank gesichert werden kann, muss dieser Wert `$$_TSMDBMGR_$$` lauten.

Achtung: Fügen Sie nicht die Option `PASSWORDACCESS generate` zur Konfigurationsdatei `dsm.sys` hinzu. Diese Option kann einen Datenbanksicherungsfehler verursachen.

5. Optional: Konfigurieren Sie den Server für die Datenbanksicherung mithilfe von Shared Memory. Auf diese Weise könnten Sie die Prozessorauslastung verringern und den Durchsatz verbessern. Führen Sie die folgenden Schritte aus:

   a. Überprüfen Sie die Datei `dsmserv.opt`. Fügen Sie die folgenden Zeilen in die Datei ein, falls nicht vorhanden:

   ```
   commmethod sharedmem
   shmport Anschlussnummer
   ```

   Hierbei steht *Anschlussnummer* für den Anschluss, der für Shared Memory verwendet werden soll.

   b. Suchen Sie in der Konfigurationsdatei `dsm.sys` die folgenden Zeilen:

   ```
   commmethod tcpip
   tcpserveraddr localhost
   tcpport Anschlussnummer
   ```

   Ersetzen Sie die angegebenen Zeilen durch die folgenden Zeilen:

   ```
   commmethod sharedmem
   shmport Anschlussnummer
   ```

   Hierbei steht *Anschlussnummer* für den Anschluss, der für Shared Memory verwendet werden soll.

Serveroptionen für die Verwaltung der Serverdatenbank konfigurieren

Um Probleme bezüglich des Datenbankwachstums und der Serverleistung zu vermeiden, überwacht der Server automatisch seine Datenbanktabellen und reorganisiert diese Tabellen, wenn dies erforderlich ist. Bevor der Server für den Produktionseinsatz gestartet wird, definieren Sie Serveroptionen, mit denen gesteuert wird, wann die Reorganisation ausgeführt wird. Ist die Verwendung der Datendeduplizierung geplant, stellen Sie sicher, dass die Option für die Ausführung der Indexreorganisation aktiviert ist.

Informationen zu diesem Vorgang

Die Tabellen- und Indexreorganisation erfordert in hohem Umfang Prozessorressourcen, Speicherbereich für die aktive Protokolldatei und Speicherbereich für das Archivprotokoll. Da die Datenbanksicherung Vorrang vor der Reorganisation hat, wählen Sie den Zeitpunkt und die Dauer für die Reorganisation aus, um sicherzustellen, dass sich die Prozesse nicht überlappen und die Reorganisation ausgeführt werden kann.

Sie können die Index- und Tabellenreorganisation für die Serverdatenbank optimieren. Auf diese Weise können Sie die Vermeidung von unerwartetem Datenbankwachstum und Leistungsproblemen verbessern. Anweisungen finden Sie in Technote 1683633.

Wenn Sie diese Serveroptionen aktualisieren, während der Server aktiv ist, müssen Sie den Server stoppen und erneut starten, damit die aktualisierten Werte wirksam werden.

Vorgehensweise

1. Ändern Sie die Serveroptionen.

   Bearbeiten Sie die Serveroptionsdatei `dsmserv.opt` im Serverinstanzverzeichnis. Beachten Sie bei der Bearbeitung der Serveroptionsdatei die folgenden Richtlinien:

   - Entfernen Sie den Stern am Zeilenanfang, um eine Option zu aktivieren.
   - Geben Sie eine Option in einer beliebigen Zeile ein.
   - Geben Sie nur eine Option pro Zeile ein. Die vollständige Option mit ihrem Wert muss sich in einer Zeile befinden.
   - Haben Sie mehrere Einträge für eine Option in der Datei, verwendet der Server den letzten Eintrag.

   Die verfügbaren Serveroptionen können Sie mit der Musterdatei `dsmserv.opt.smp` im Verzeichnis `/opt/tivoli/tsm/server/bin` anzeigen.
2. Ist die Verwendung der Datendeduplizierung geplant, aktivieren Sie die Serveroption **ALLOWREORGINDEX**.

   Fügen Sie der Serveroptionsdatei die folgende Option und den folgenden Wert hinzu:

   ```
   allowreorgindex yes
   ```
3. Definieren Sie die Serveroptionen **REORGBEGINTIME** und **REORGDURATION**, mit denen gesteuert wird, wann die Reorganisation gestartet und wie lange sie ausgeführt wird. Wählen Sie den Zeitpunkt und die Dauer so aus, dass die Reorganisation ausgeführt wird, wenn der Server voraussichtlich am wenigsten ausgelastet ist.

   Diese Serveroptionen steuern sowohl die Tabellen- als auch die Indexreorganisationsprozesse.

   a) Definieren Sie die Startzeit der Reorganisation mit der Serveroption **REORGBEGINTIME**. Geben Sie die Zeit im 24-Stunden-Format an.
   Um beispielsweise als Startzeit der Reorganisation 20:30 Uhr festzulegen, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:

   ```
   reorgbegintime 20:30
   ```

   b) Definieren Sie das Intervall, in dem der Server die Reorganisation starten kann.
   Um beispielsweise anzugeben, dass der Server die Reorganisation innerhalb von 4 Stunden nach dem mit der Serveroption **REORGBEGINTIME** definierten Zeitpunkt starten kann, geben Sie die folgende Option und den folgenden Wert in der Serveroptionsdatei an:

   ```
   reorgduration 4
   ```
4. War der Server aktiv, während Sie die Serveroptionsdatei aktualisiert haben, stoppen Sie den Server und starten Sie ihn erneut.

Serverinstanz starten

Sie können den Server mit der Instanzbenutzer-ID (bevorzugte Methode) oder mit der Rootbenutzer-ID starten.

Vorbereitende Schritte

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden.

Informationen zu diesem Vorgang

Wenn Sie den Server unter Verwendung der Instanzbenutzer-ID starten, wird der Konfigurationsprozess vereinfacht und potenzielle Probleme werden vermieden. In einigen Fällen kann jedoch die Verwendung der Rootbenutzer-ID zum Starten des Servers erforderlich sein. Beispielsweise kann die Rootbenutzer-ID verwendet werden, um sicherzustellen, dass der Server auf bestimmte Einheiten zugreifen kann. Sie können den automatischen Serverstart mit der Instanzbenutzer-ID oder mit der Rootbenutzer-ID konfigurieren.

Wenn Sie Verwaltungs- oder Rekonfigurationstasks ausführen müssen, starten Sie den Server im Verwaltungsmodus.

Vorgehensweise

Führen Sie einen der folgenden Schritte aus, um den Server zu starten:

- Starten Sie den Server mithilfe der Instanzbenutzer-ID.

  Anweisungen siehe „Server mit der Instanzbenutzer-ID starten" auf Seite 105.
- Starten Sie den Server mithilfe der Rootbenutzer-ID.

  Anweisungen zum Berechtigen von Rootbenutzer-IDs zum Starten des Servers finden Sie in Rootbenutzer-IDs zum Starten des Servers berechtigen (Version 7.1.1). Anweisungen zum Starten des Servers mit der Rootbenutzer-ID finden Sie in Server mit der Rootbenutzer-ID starten (Version 7.1.1).
- Starten Sie den Server automatisch.

  Anweisungen siehe „Server auf Linux-Systemen automatisch starten" auf Seite 105.
- Starten Sie den Server im Verwaltungsmodus.

  Anweisungen siehe „Server im Verwaltungsmodus starten" auf Seite 107.

Zugriffsberechtigungen und Benutzergrenzwerte überprüfen

Vor dem Start des Servers überprüfen Sie Zugriffsberechtigungen und Benutzergrenzwerte.

Informationen zu diesem Vorgang

Wenn Sie die Benutzergrenzwerte, die auch als *ulimit-Werte* bezeichnet werden, nicht überprüfen, kann dies dazu führen, dass der Server instabil wird oder nicht antworten kann. Die müssen auch den systemweiten Grenzwert für die maximale Anzahl offener Dateien überprüfen. Der systemweite Grenzwert muss größer-gleich dem Benutzergrenzwert sein.

Vorgehensweise

1. Überprüfen Sie, ob die Benutzer-ID der Serverinstanz über Berechtigungen zum Starten des Servers verfügt.
2. Stellen Sie für die Serverinstanz, die Sie starten wollen, sicher, dass Sie über die Berechtigung zum Lesen und Schreiben von Dateien im Serverinstanzverzeichnis verfügen.

   Stellen Sie sicher, dass die Datei `dsmserv.opt` im Serverinstanzverzeichnis vorhanden ist und dass die Datei Parameter für die Serverinstanz enthält.
3. Wenn der Server mit einem Bandlaufwerk, einem Datenträgerwechsler oder mit einer Einheit für austauschbare Datenträger verbunden ist und Sie den Server mit der Instanzbenutzer-ID starten wollen, erteilen Sie der Instanzbenutzer-ID Schreib-/Lesezugriff für diese Einheiten. Führen Sie einen der folgenden Schritte aus, um Berechtigungen festzulegen:

- Bei einem für IBM Spectrum Protect dediziertem System, auf das nur der IBM Spectrum Protect-Administrator zugreifen kann, erteilen Sie globale Schreibberechtigung für die Gerätedateien der Einheiten. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

  ```
  chmod +w /dev/rmtX
  ```

- Verfügt das System über mehrere Benutzer, können Sie den Zugriff einschränken, indem Sie die IBM Spectrum Protect-Instanzbenutzer-ID zum Eigner der Gerätedateien der Einheit machen. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

  ```
  chmod u+w /dev/rmtX
  ```

- Sind mehrere Benutzerinstanzen auf einem System aktiv, ändern Sie den Gruppennamen (z. B. TAPEUSERS) und fügen Sie jede IBM Spectrum Protect-Instanzbenutzer-ID dieser Gruppe hinzu. Übertragen Sie dann das Eigentumsrecht der Gerätedateien der Einheiten an die Gruppe TAPEUSERS und erteilen Sie Schreibberechtigung für die Gruppe. Geben Sie den folgenden Befehl in der Befehlszeile des Betriebssystems aus:

  ```
  chmod g+w /dev/rmtX
  ```

4. Wenn Sie den IBM Spectrum Protect-Einheitentreiber und das Dienstprogramm **autoconf** verwenden, erteilen Sie der Instanzbenutzer-ID mithilfe der Option **-a** Schreib-/Lesezugriff.
5. Um Serverfehler während der Interaktion mit IBM Db2 zu verhindern, optimieren Sie die Kernelparameter.

   Anweisungen zur Optimierung von Kernelparametern finden Sie in Kernelparameter optimieren.
6. Überprüfen Sie die folgenden Benutzergrenzwerte anhand der Richtlinien in der Tabelle.

Tabelle 20. Benutzergrenzwerte (ulimit-Werte)

Typ des Benutzergrenzwerts	Bevorzugter Wert	Befehl zum Abfragen des Werts
Maximale Größe der erstellten Kerndateien	Unlimited	`ulimit -Hc`
Maximale Größe eines Datensegments für einen Prozess	Unlimited	`ulimit -Hd`
Maximale Dateigröße	Unlimited	`ulimit -Hf`
Maximale Anzahl offener Dateien	65536	`ulimit -Hn`
Maximale Prozessorzeit in Sekunden	Unlimited	`ulimit -Ht`

Für die Änderung von Benutzergrenzwerten befolgen Sie die Anweisungen in der Dokumentation Ihres Betriebssystems.

Tipp: Wenn Sie den Server mithilfe eines Scripts automatisch starten wollen, können Sie die Benutzergrenzwerte in dem Script definieren.

7. Stellen Sie sicher, dass als Benutzergrenzwert für die maximale Anzahl Benutzerprozesse (`nproc`-Einstellung) der empfohlene Mindestwert 16384 festgelegt wird.
   a) Geben Sie den Befehl `ulimit -Hu` mithilfe der Instanzbenutzer-ID aus, um den aktuellen Benutzergrenzwert zu überprüfen.
   Beispiel:

   ```
   [user@Machine ~]$ ulimit -Hu
   16384
   ```

   b) Lautet der Grenzwert für die maximale Anzahl Benutzerprozesse nicht 16384, geben Sie den Wert 16384 an.

Fügen Sie der Datei /etc/security/limits.conf die folgende Zeile hinzu:

```
Instanzbenutzer-ID        -    nproc          16384
```

Hierbei gibt *Instanzbenutzer-ID* die Benutzer-ID der Serverinstanz an.

Wenn der Server im Betriebssystem Red Hat Enterprise Linux 6 installiert ist, legen Sie den Benutzergrenzwert durch Bearbeitung der Datei /etc/security/limits.d/90-nproc.conf im Verzeichnis /etc/security/limits.d fest. Diese Datei überschreibt die Einstellungen in der Datei /etc/security/limits.conf.

Tipp: Der Standardbenutzergrenzwert für die maximale Anzahl der Benutzerprozesse hat sich bei einigen Versionen des Betriebssystems Linux geändert. Der Standardwert ist 1024. Wenn Sie diesen Wert nicht durch den empfohlenen Mindestwert 16384 ersetzen, kann es zu einem Fehler oder einer Blockierung des Servers kommen.

Server mit der Instanzbenutzer-ID starten

Um den Server mit der Instanzbenutzer-ID zu starten, melden Sie sich mit der Instanzbenutzer-ID an und geben Sie im Serverinstanzverzeichnis den entsprechenden Befehl aus.

Vorbereitende Schritte

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden.

Vorgehensweise

1. Melden Sie sich an dem System, auf dem IBM Spectrum Protect installiert ist, unter Verwendung der Instanzbenutzer-ID für den Server an.
2. Wenn Sie über kein Benutzerprofil zur Ausführung des Scripts db2profile verfügen, geben Sie den folgenden Befehl aus:

   ```
   . /home/tsminst1/sqllib/db2profile
   ```

   Tipp: Anweisungen zur Aktualisierung des Benutzer-ID-Anmeldescripts zur automatischen Ausführung des Scripts db2profile finden Sie in der Db2-Produktinformation.
3. Starten Sie den Server, indem Sie den folgenden Befehl in einer einzigen Zeile im Serverinstanzverzeichnis ausgeben:

   ```
   usr/bin/dsmserv
   ```

   Tipp: Der Befehl wird im Vordergrund ausgeführt, sodass Sie eine Administrator-ID definieren und der Serverinstanz zuordnen können.

   Hat beispielsweise die Serverinstanz den Namen tsminst1 und das Serverinstanzverzeichnis den Namen /tsminst1, können Sie die Instanz starten, indem Sie die folgenden Befehle ausgeben:

   ```
   cd /tsminst1
    . ~/sqllib/db2profile
   /usr/bin/dsmserv
   ```

Server auf Linux-Systemen automatisch starten

Um einen Server unter einem Linux-Betriebssystem automatisch zu starten, verwenden Sie das Script **dsmserv.rc**.

Vorbereitende Schritte

Stellen Sie sicher, dass Kernelparameter korrekt definiert werden.

Stellen Sie sicher, dass die Serverinstanz mit der Benutzer-ID des Instanzeigners ausgeführt wird.

Stellen Sie sicher, dass Zugriffsberechtigungen und Benutzergrenzwerte korrekt definiert werden.

Informationen zu diesem Vorgang

Das Script **dsmserv.rc** befindet sich im Serverinstallationsverzeichnis, beispielsweise `/opt/tivoli/tsm/server/bin`.

Das Script **dsmserv.rc** kann entweder zum manuellen Starten des Servers oder zum automatischen Starten des Servers verwendet werden, indem dem Verzeichnis `/etc/rc.d/init.d` Einträge hinzugefügt werden. Das Script wird zusammen mit Linux-Dienstprogrammen wie **CHKCONFIG** und **SERVICE** eingesetzt.

Vorgehensweise

Führen Sie für jede Serverinstanz, die automatisch gestartet werden soll, die folgenden Schritte aus:

1. Stellen Sie eine Kopie des Scripts **dsmserv.rc** in das Verzeichnis `/init.d`, beispielsweise `/etc/rc.d/init.d`.

   Stellen Sie sicher, dass Sie nur die Kopie des Scripts ändern. Ändern Sie nicht das ursprüngliche Script!
2. Benennen Sie die Kopie des Scripts so um, dass sie dem Namen des Serverinstanzeigners entspricht, beispielsweise `tsminst1`.

   Das Script wurde unter der Voraussetzung erstellt, dass das Serverinstanzverzeichnis *Ausgangsverzeichnis*`/tsminst1` ist, beispielsweise `/home/tsminst1/tsminst1`.
3. Wenn das Serverinstanzverzeichnis nicht *Ausgangsverzeichnis*`/tsminst1` ist, suchen Sie in der Kopie des Scripts nach der folgenden Zeile:

   ```
   instance_dir="${Instanzausgangsverzeichnis}/tsminst1"
   ```

   Ändern Sie die Zeile so, dass sie auf Ihr Serverinstanzverzeichnis verweist, beispielsweise:

   ```
   instance_dir="/tsminst1"
   ```
4. Lokalisieren Sie in der Kopie des Scripts die folgende Zeile:

   ```
   # pidfile: /var/run/dsmserv_Instanzname_su.pid
   ```

   Ändern Sie den Wert für den Instanznamen in den Namen des Serverinstanzeigners.

   Wenn beispielsweise der Serverinstanzeigner den Namen tsminst1 hat, aktualisieren Sie die Zeile wie folgt:

   ```
   # pidfile: /var/run/dsmserv_tsminst1_su.pid
   ```
5. Konfigurieren Sie die Ausführungsebene, auf der der Server automatisch gestartet wird. Verwenden Sie Tools wie das Dienstprogramm **CHKCONFIG**, um einen Wert anzugeben, der einem Mehrbenutzermodus mit aktiviertem Netzbetrieb entspricht. Normalerweise ist der zu verwendende Wert für die Ausführungsebene abhängig vom Betriebssystem und seiner Konfiguration 3 oder 5. Weitere Informationen zum Mehrbenutzermodus und zu Ausführungsebenen enthält die Dokumentation zu Ihrem Betriebssystem.
6. Um den Server zu starten oder zu stoppen, geben Sie einen der folgenden Befehle aus:
   - Zum Starten des Servers:

     ```
     service tsminst1 start
     ```
   - Zum Stoppen des Servers:

     ```
     service tsminst1 stop
     ```

Beispiel

In diesem Beispiel werden die folgenden Werte verwendet:

- Der Instanzeigner ist tsminst1.
- Das Serverinstanzverzeichnis ist /home/tsminst1/tsminst1.
- Die Kopie des Scripts **dsmserv.rc** hat den Namen tsminst1.
- Das Dienstprogramm **CHKCONFIG** wird verwendet, um das Starten des Scripts auf den Ausführungsebenen 3, 4 und 5 zu konfigurieren.

```
cp /opt/tivoli/tsm/server/bin/dsmserv.rc /etc/rc.d/init.d/tsminst1
sed -i 's/dsmserv_Instanzname.pid/dsmserv_tsminst1.pid/' /etc/rc.d/init.d/tsminst1
chkconfig --list tsminst1
service tsminst1 supports chkconfig, but is not referenced in
any runlevel (run 'chkconfig --add tsminst1')
chkconfig --add tsminst1
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:off 4:off 5:off 6:off
chkconfig --level 345 tsminst1 on
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:on 4:on 5:on 6:off
```

Server im Verwaltungsmodus starten

Sie können den Server im Verwaltungsmodus starten, um Unterbrechungen während Verwaltungs- oder Rekonfigurationstasks zu vermeiden.

Informationen zu diesem Vorgang

Starten Sie den Server im Verwaltungsmodus, indem Sie das Dienstprogramm **DSMSERV** mit dem Parameter **MAINTENANCE** ausführen.

Im Verwaltungsmodus sind die folgenden Operationen inaktiviert:

- Zeitpläne für Verwaltungsbefehle
- Clientzeitpläne
- Konsolidierung von Speicherbereich auf dem Server
- Bestandsverfall
- Umlagerung von Speicherpools

Darüber hinaus wird verhindert, dass Clients Sitzungen mit dem Server starten können.

Tipps:

- Sie müssen die Serveroptionsdatei, dsmserv.opt, nicht editieren, um den Server im Verwaltungsmodus starten zu können.
- Während der Server im Verwaltungsmodus ausgeführt wird, können Sie die Speicherbereichskonsolidierung (-wiederherstellung), den Bestandsverfall und Umlagerungsprozesse für Speicherpools manuell starten.

Prozedur

- Um den Server im Verwaltungsmodus zu starten, geben Sie den folgenden Befehl aus:

  ```
  dsmserv maintenance
  ```

  Tipp: Ein Video zum Starten des Servers im Verwaltungsmodus kann über Server im Verwaltungsmodus starten angezeigt werden.

Nächste Schritte

Um Serveroperationen im Produktionsmodus wiederaufzunehmen, führen Sie die folgenden Schritte aus:

1. Fahren Sie den Server herunter, indem Sie den Befehl **HALT** ausgeben:

```
halt
```

2. Starten Sie den Server mithilfe der Methode, die Sie im Produktionsmodus verwenden.

Operationen, die im Verwaltungsmodus inaktiviert waren, werden wieder aktiviert.

Server stoppen

Sie können den Server bei Bedarf stoppen, um die Steuerung an das Betriebssystem zurückzugeben. Um den Verlust von Verwaltungs- und Clientknotenverbindungen zu vermeiden, stoppen Sie den Server erst nach Beendigung oder Abbruch laufender Sitzungen.

Informationen zu diesem Vorgang

Geben Sie den folgenden Befehl in die IBM Spectrum Protect-Befehlszeile ein, um den Server zu stoppen:

```
halt
```

Wenn Sie keine Verbindung zum Server mit einem Verwaltungsclient herstellen können und wenn der Server gestoppt werden soll, müssen Sie den Prozess mit dem Befehl **kill** mit der Prozess-ID (PID) abbrechen. Die PID wird bei der Initialisierung angezeigt.

Wichtig: Bevor der Befehl **kill** eingegeben wird, müssen Sie sicherstellen, dass die korrekte Prozess-ID für den IBM Spectrum Protect-Server bekannt ist.

Die Prozess-ID des mit dem Befehl kill abzubrechenden Prozesses kann mithilfe der Datei `dsmserv.v6lock` in dem Verzeichnis, in dem der Server ausgeführt wird, ermittelt werden. Geben Sie Folgendes ein, um die Datei anzuzeigen:

```
cat /instance_dir/dsmserv.v6lock
```

Geben Sie den folgenden Befehl aus, um den Server zu stoppen:

```
kill -23 dsmserv_pid
```

Hierbei steht *dsmserv_pid* für die Prozess-ID.

Lizenzregistrierung

Registrieren Sie alle lizenzierten IBM Spectrum Protect-Funktionen, die Sie beziehen, sofort, damit Sie nach dem Starten der Serveroperationen (z. B. Datensicherung) keine Daten verlieren.

Informationen zu diesem Vorgang

Verwenden Sie hierfür den Befehl **REGISTER LICENSE**.

Beispiel: Lizenz registrieren

Die IBM Spectrum Protect-Basislizenz registrieren.

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

Server für Datenbanksicherungsoperationen vorbereiten

Sie müssen eine Einheitenklasse für Band (tape), Datei (file) oder Cloud (cloud) angeben und andere Schritte ausführen, um den Server für automatische und manuelle Datenbanksicherungsoperationen vorzubereiten.

Vorgehensweise

1. Stellen Sie sicher, dass die IBM Spectrum Protect-Serverkonfiguration abgeschlossen ist.

   Tipp: Sie können den Server für Datenbanksicherungen mithilfe des Konfigurationsassistenten (`dsmicfgx`) konfigurieren oder Sie können die Schritte manuell ausführen. Weitere Informationen zur Konfiguration finden Sie im Abschnitt *Server konfigurieren* im IBM Knowledge Center.
2. Wählen Sie die Einheitenklasse aus, die für Datenbanksicherungen verwendet werden soll, schützen Sie den Masterverschlüsselungsschlüssel und definieren Sie ein Kennwort.

   Stellen Sie sicher, dass die folgenden Schlüsseldateien geschützt sind:

   - Masterverschlüsselungsschlüsseldateien (dsmkeydb.*)
   - Dateien mit Serverzertifikaten und privaten Schlüsseln (cert.*)

   Geben Sie den Befehl **SET DBRECOVERY** in der Verwaltungsbefehlszeile aus, um diese Aktionen auszuführen:

   ```
   set dbrecovery Einheitenklassenname protectkeys=yes password=Kennwortname
   ```

   Dabei gibt *Einheitenklassenname* die für Datenbanksicherungsoperationen zu verwendende Einheitenklasse und *Kennwortname* das Kennwort an.

   Sie müssen einen Einheitenklassennamen angeben; andernfalls schlägt die Sicherung fehl. Durch die Angabe von **PROTECTKEYS=YES** wird sichergestellt, dass der Masterverschlüsselungsschlüssel während der Ausführung von Datenbanksicherungsoperationen gesichert wird. Für Cloudeinheitenklassen ist der Parameter **PROTECTKEYS=YES** erforderlich.

   Erstellen Sie ein sicheres Kennwort, das mindestens 8 Zeichen lang ist. Wenn Sie ein Kennwort für die Datenbanksicherung angeben, müssen Sie dasselbe Kennwort im Befehl **RESTORE DB** angeben, um die Datenbank zurückzuschreiben.

   Achtung: Sie dürfen das Kennwort nicht vergessen und eine Kopie an einem sicheren Ort aufbewahren. Ohne das Kennwort ist eine Datenwiederherstellung nicht möglich.

Beispiel

Um anzugeben, dass Datenbanksicherungen eine Kopie des Masterverschlüsselungsschlüssels für den Server einschließen sollen, führen Sie den folgenden Befehl aus:

```
set dbrecovery dbback protectkeys=yes password=protect8991
```

Mehrere Serverinstanzen auf einem System ausführen

Sie können mehrere Serverinstanzen auf Ihrem System erstellen. Jede Serverinstanz verfügt über ein eigenes Instanzverzeichnis sowie über Datenbank- und Protokollverzeichnisse.

Multiplizieren Sie den Speicherbedarf und andere Systemvoraussetzungen für einen Server mit der geplanten Instanzzahl für das System.

Die Gruppe der Dateien für eine Instanz des Servers wird getrennt von den Dateien gespeichert, die von einer anderen Serverinstanz auf demselben System verwendet werden. Gehen Sie für jede neue Instanz wie im Abschnitt über die Erstellung der Serverinstanz beschrieben vor, einschließlich der Erstellung des neuen Instanzbenutzers.

Zur Verwaltung des von jedem Server verwendeten Systemspeichers begrenzen Sie mit der Serveroption DBMEMPERCENT den Prozentsatz des Systemspeichers. Haben alle Server denselben Stellenwert, verwenden Sie für jeden Server denselben Wert. Ist ein Server ein Produktionsserver und andere Server sind Testserver, geben Sie für den Produktionsserver einen höheren Wert an als für die Testserver.

Von Version 7.1 auf Version 8.1 ist ein direktes Upgrade möglich. Weitere Informationen finden Sie im Abschnitt über das Upgrade. Wenn Sie ein Upgrade durchführen und mehrere Server auf dem System haben,

müssen Sie den Installationsassistenten nur einmal ausführen. Der Installationsassistent erfasst die Datenbank- und Variablendaten für alle ursprünglichen Serverinstanzen.

Server überwachen

Wenn Sie den Server im Produktionsbetrieb einsetzen, überwachen Sie den von ihm verwendeten Speicherbereich, um sicherzustellen, dass die Größe des Speicherbereichs angemessen ist. Ändern Sie den Speicherbereich, falls erforderlich.

Vorgehensweise

1. Überwachen Sie die aktive Protokolldatei, um sicherzustellen, dass die Größe für die Auslastung der Serverinstanz korrekt ist.

   Wenn die Serverauslastung ihren normalen erwarteten Stand erreicht hat, belegt der von der aktiven Protokolldatei verwendete Speicherbereich 80 bis 90 Prozent des Speicherbereichs, der für das Verzeichnis für aktive Protokolldateien zur Verfügung steht. An diesem Punkt müssen Sie den Speicherbereich möglicherweise vergrößern. Die Vergrößerung des Speicherbereichs ist von der Art der Transaktionen in der Serververarbeitung abhängig. Transaktionsmerkmale wirken sich auf die Belegung des Speicherbereichs der aktiven Protokolldateien aus.

   Die folgenden Transaktionsmerkmale können sich auf die Speicherbereichsbelegung in der aktiven Protokolldatei auswirken:

   - Die Anzahl und Größe der Dateien in Sicherungsoperationen
     - Clients, wie z. B. Dateiserver, die zahlreiche kleine Dateien sichern, können zahlreiche Transaktionen verursachen, die in kurzer Zeit ausgeführt werden. Die Transaktionen können sehr viel Speicherbereich in der aktiven Protokolldatei belegen, jedoch nur für kurze Zeit.
     - Clients, wie z. B. E-Mail-Server oder ein Datenbankserver, die große Datenvolumen in wenigen Transaktionen sichern, können wenige Transaktionen verursachen, deren Auführung viel Zeit in Anspruch nimmt. Die Transaktionen können wenig Speicherbereich in der aktiven Protokolldatei belegen, jedoch für lange Zeit.
   - Netzverbindungstypen
     - Mit schnellen Netzverbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, die schneller ausgeführt werden. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen kürzeren Zeitraum.
     - Mit langsameren Verbindungen ausgeführte Sicherungsoperationen verursachen Transaktionen, deren Ausführung länger dauert. Die Transaktionen belegen Speicherbereich in der aktiven Protokolldatei über einen längeren Zeitraum.

   Wenn der Server Transaktionen mit sehr unterschiedlichen Merkmalen verarbeitet, kann der für die aktive Protokolldatei verwendete Speicherbereich im Lauf der Zeit sehr stark schwanken. Für einen solchen Server müssen Sie unter Umständen dafür sorgen, dass ein niedrigerer Prozentsatz des Speicherbereichs der aktiven Protokolldatei verwendet wird. Der zusätzliche Speicherbereich gestattet eine Vergrößerung der aktiven Protokolldatei für Transaktionen, die viel Zeit in Anspruch nehmen.
2. Überwachen Sie das Archivprotokoll, um sicherzustellen, dass immer Speicherbereich verfügbar ist.

   Hinweis: Wenn das Archivprotokoll und das Übernahmearchivprotokoll voll werden, kann die aktive Protokolldatei voll werden, so dass der Server stoppt. Für das Archivprotokoll muss so viel Speicherbereich zur Verfügung stehen, dass dieser niemals vollständig belegt wird.

   Sie werden wahrscheinlich Folgendes feststellen:

   a. Am Anfang wird das Archivprotokoll schnell größer, wenn normale Clientsicherungsoperationen ausgeführt werden.
   b. Datenbanksicherungen werden regelmäßig ausgeführt, entweder mit einem Zeitplan oder manuell.

c. Nach mindestens zwei Datenbankgesamtsicherungen wird das Abschneiden des Protokolls automatisch ausgeführt. Der vom Archivprotokoll belegte Speicherbereich verringert sich durch das Abschneiden.

d. Normale Clientoperationen werden fortgesetzt und das Archivprotokoll wird wieder größer.

e. Datenbanksicherungen finden regelmäßig statt und die Häufigkeit der Protokollbereinigung ist von der Häufigkeit der Datenbankgesamtsicherungen abhängig.

Nach diesem Muster nimmt die Größe des Archivprotokolls zunächst zu, verringert sich und nimmt dann eventuell wieder zu. Im Laufe der Zeit sollte der vom Archivprotokoll belegte Speicherbereich während der normalen Verarbeitung einen relativ konstanten Stand erreichen.

Wenn die Größe des Archivprotokolls weiter zunimmt, sollten Sie eine oder beide der folgenden Maßnahmen in Betracht ziehen:

- Ordnen Sie dem Archivprotokoll weiteren Speicherbereich zu. Sie müssen unter Umständen das Archivprotokoll in ein anderes Dateisystem versetzen.
- Erhöhen Sie die Häufigkeit der Datenbankgesamtsicherungen, so dass die Protokollbereinigung häufiger stattfindet.

3. Wenn Sie ein Verzeichnis für das Übernahmearchivprotokoll definiert haben, überprüfen Sie, ob darin Protokolle während der normalen Verarbeitung gespeichert werden. Wenn der Speicherbereich des Übernahmeprotokolls verwendet wird, sollten Sie das Archivprotokoll vergrößern.

   Das Übernahmearchivprotokoll sollte nur unter außergewöhnlichen Bedingungen verwendet werden, nicht während der normalen Verarbeitung.

Kapitel 4. IBM Spectrum Protect-Server-Fixpack installieren

IBM Spectrum Protect-Wartungsaktualisierungen (werden auch als Fixpacks bezeichnet) bringen Ihren Server auf die aktuelle Wartungsstufe.

Vorbereitende Schritte

Damit ein Fixpack oder ein vorläufiger Fix auf dem Server installiert werden kann, müssen Sie den Server mit der Stufe installieren, auf der er ausgeführt werden soll. Sie müssen die Serverinstallation nicht mit dem Basisrelease beginnen. Wenn momentan beispielsweise Version 8.1.1 installiert ist, können Sie das aktuelle Fixpack für Version 8.1 direkt verwenden. Sie müssen nicht mit der Installation von Version 8.1.0 beginnen, wenn eine Wartungsaktualisierung verfügbar ist.

Das IBM Spectrum Protect-Lizenzpaket muss installiert sein. Das Lizenzpaket wird beim Kauf eines Basisreleases bereitgestellt. Wenn Sie ein Fixpack oder einen vorläufigen Fix von Fix Central herunterladen, installieren Sie die Serverlizenz, die auf der Website von Passport Advantage zur Verfügung steht. Sollen Nachrichten und Hilfetext nicht in Englisch angezeigt werden, installieren Sie das gewünschte Sprachenpaket.

Wenn Sie ein Upgrade des Servers durchführen und den Server dann auf einen früheren Stand zurücksetzen, müssen Sie die Datenbank auf einen Zeitpunkt vor dem Upgrade zurückschreiben. Führen Sie während des Upgrades die erforderlichen Schritte aus, mit denen sichergestellt wird, dass die Datenbank zurückgeschrieben werden kann: Sichern Sie die Datenbank, die Protokolldatei für Datenträger, die Einheitenkonfigurationsdatei und die Serveroptionsdatei.

Wenn Sie den Clientverwaltungsservice verwenden, müssen Sie ein Upgrade dieses Service auf dieselbe Version wie beim IBM Spectrum Protect-Server durchführen.

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease des installierten Servers aufbewahrt werden. Wenn Sie IBM Spectrum Protect über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, sind die Installationsmedien für das Basisrelease des Servers für die Neuinstallation der Lizenz erforderlich.

Rufen Sie das IBM Support Portal auf. Hier finden Sie folgende Informationen:

- Eine Liste der neuesten Wartungs- und Download-Fixes. Klicken Sie auf **Download** und legen Sie alle gültigen Fixes an.
- Informationen zum Erwerb eines Basislizenzpakets. Suchen Sie nach **Downloads > Passport Advantage**.
- Unterstützte Plattformen und Systemvoraussetzungen. Suchen Sie nach **IBM Spectrum Protect supported operating systems**.

Sie müssen ein Upgrade des Servers durchführen, bevor Sie ein Upgrade der Clients für Sichern/Archivieren durchführen. Wenn Sie das Upgrade des Servers nicht zuerst durchführen, könnte die Kommunikation zwischen dem Server und den Clients unterbrochen werden.

Achtung: Sie dürfen die Db2-Software, die mit den IBM Spectrum Protect-Installationspaketen und -Fixpacks installiert wird, nicht ändern. Installieren Sie keine andere Version, kein anderes Release oder Fixpack der Db2-Software und führen Sie kein Upgrade durch, da dies die Datenbank beschädigen kann.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Fixpack oder einen vorläufigen Fix zu installieren:

1. Sichern Sie die Datenbank. Die bevorzugte Methode ist eine Momentaufnahmesicherung. Bei einer Momentaufnahmesicherung handelt es sich um eine Datenbankgesamtsicherung, bei der geplante Datenbanksicherungen nicht unterbrochen werden. Geben Sie beispielsweise den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```

2. Sichern Sie die Einheitenkonfigurationsdaten. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

   ```
   backup devconfig filenames=Dateiname
   ```

   Dateiname gibt den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.

3. Speichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis oder benennen Sie die Datei um. Geben Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus:

   ```
   backup volhistory filenames=Dateiname
   ```

   Dateiname gibt den Namen der Datei an, in der Datenträgerhistory-Informationen (Datenträgerprotokolldaten) gespeichert werden sollen.

4. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise `dsmserv.opt` heißt. Die Datei befindet sich im Serverinstanzverzeichnis.
5. Halten Sie den Server vor der Installation eines Fixpacks oder eines vorläufigen Fixes an.

   Verwenden Sie den Befehl **HALT**.

6. Stellen Sie sicher, dass im Installationsverzeichnis zusätzlicher Speicherplatz zur Verfügung steht.

   Für die Installation dieses Fixpacks kann zusätzlicher temporärer Plattenspeicherplatz im Installationsverzeichnis des Servers erforderlich sein. Die Größe des zusätzlichen Plattenspeicherplatzes kann der Größe entsprechen, die für die Installation einer neuen Datenbank während einer IBM Spectrum Protect-Installation benötigt wird. Der IBM Spectrum Protect-Installationsassistent zeigt an, wie viel Speicherplatz für die Installation des Fixpacks benötigt wird und wie viel Platz zur Verfügung steht. Wenn der erforderliche Speicherplatz größer ist als der verfügbare Speicherplatz, stoppt die Installation. Wenn die Installation stoppt, fügen Sie dem Dateisystem den erforderlichen Plattenspeicherplatz hinzu und starten Sie die Installation erneut.

7. Melden Sie sich als Root an.
8. Laden Sie die Paketdatei für das Fixpack bzw. den vorläufigen Fix, das bzw. der installiert werden soll, über IBM Support Portal, Passport Advantage oder Fix Central herunter.
9. Wechseln Sie in das Verzeichnis, in dem sich die ausführbare Datei befindet, und führen Sie die folgenden Schritte aus.

   Tipp: Die Dateien werden in das aktuelle Verzeichnis extrahiert. Stellen Sie sicher, dass sich die ausführbare Datei in dem Verzeichnis befindet, in dem sich die extrahierten Dateien befinden sollen.

   a. Geben Sie den folgenden Befehl ein, um die Dateiberechtigungen zu ändern:

      ```
      chmod a+x 8.x.x.x-IBM-SPSRV-Plattform.bin
      ```

      Hierbei steht *Plattform* für die Architektur, in der IBM Spectrum Protect installiert werden soll.

   b. Geben Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

      ```
      ./8.x.x.x-IBM-SPSRV-Plattform.bin
      ```

10. Wählen Sie eine der folgenden Möglichkeiten für die Installation von IBM Spectrum Protect aus.

    Wichtig: Nach der Installation eines Fixpacks muss die Konfiguration nicht wiederholt werden. Sie können nach Beendigung der Installation stoppen, alle Fehler beheben und dann Ihre Server erneut starten.

    Installieren Sie die IBM Spectrum Protect-Software mit einer der folgenden Methoden:

Installationsassistent
Befolgen Sie die Anweisungen für Ihr Betriebssystem:

„IBM Spectrum Protect mit dem Installationsassistenten installieren" auf Seite 84

Tipp: Klicken Sie nach dem Start des Assistenten im Fenster von **IBM Installation Manager** auf das Symbol **Aktualisieren**. Klicken Sie nicht auf das Symbol **Installieren** oder **Ändern**.

Befehlszeile im Konsolenmodus
Befolgen Sie die Anweisungen für Ihr Betriebssystem:

„IBM Spectrum Protect im Konsolenmodus installieren" auf Seite 85

Tipp: Befinden sich mehrere Serverinstanzen auf Ihrem System, führen Sie den Installationsassistenten nur einmal aus. Der Installationsassistent führt ein Upgrade aller Serverinstanzen durch.

Ergebnisse

Beheben Sie alle Fehler, die während des Installationsprozesses festgestellt werden.

Wenn Sie den Server mithilfe des Installationsassistenten installiert haben, können Sie Installationsprotokolle mithilfe des Tools IBM Installation Manager anzeigen. Klicken Sie auf **Datei** > **Protokoll anzeigen**. Um Protokolldateien zu erfassen, klicken Sie in IBM Installation Manager auf **Hilfe** > **Daten zur Fehleranalyse exportieren**.

Wenn Sie den Server im Konsolenmodus oder im unbeaufsichtigten Modus installiert haben, können Sie Fehlerprotokolle im IBM Installation Manager-Protokollverzeichnis anzeigen. Zum Beispiel:

```
/var/ibm/InstallationManager/logs
```

Kapitel 5. Upgrade auf Version 8.1 durchführen

Führen Sie ein Upgrade des IBM Spectrum Protect-Servers durch, damit neue Produktfunktionen und Aktualisierungen genutzt werden können.

Vorbereitende Schritte

Lesen Sie die Planungsinformationen für die Sicherheitsupdates in „Was Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten" auf Seite 3.

Informationen zu diesem Vorgang

Informationen zum Upgrade des Servers auf demselben Betriebssystem finden Sie in den Upgradeanweisungen. Anweisungen zur Migration des Servers in ein anderes Betriebssystem finden Sie in IBM Spectrum Protect Upgrade and Migration Process - Frequently Asked Questions.

Tabelle 21. Upgradeanweisungen

Upgrade von Version	Auf Version	Siehe
Version 8.1	Version 8.1, Fixpack oder vorläufiger Fix	Kapitel 4, „IBM Spectrum Protect-Server-Fixpack installieren", auf Seite 113
Version 7.1	Version 8.1	„Server installieren und Upgrade prüfen" auf Seite 120
Version 7.1	Version 8.1, Fixpack oder vorläufiger Fix	Kapitel 4, „IBM Spectrum Protect-Server-Fixpack installieren", auf Seite 113
Version 5.5, 6.2 oder 6.3	Version 8.1	IBM Spectrum Protect Upgrade and Migration Process - Frequently Asked Questions

Ein Upgrade von Version 7 auf Version 8.1 dauert ca. 20 - 50 Minuten. Die Ergebnisse in Ihrer Umgebung können von den im Labor erzielten Ergebnissen abweichen.

Informationen zu Upgrades in einer Clusterumgebung finden Sie in „Server-Upgrade in einer Clusterumgebung durchführen" auf Seite 123.

Soll nach einem Upgrade oder einer Migration auf eine frühere Version des Servers zurückgesetzt werden, benötigen Sie eine Datenbankgesamtsicherung und die Installationssoftware für den ursprünglichen Server. Sie benötigen außerdem die folgenden Schlüsselkonfigurationsdateien:

- Protokolldatei für Datenträger
- Einheitenkonfigurationsdatei
- Serveroptionsdatei

Zugehörige Informationen

IBM Spectrum Protect-Upgrade- und -Migrationsprozess - Häufig gestellte Fragen

Upgrade auf Version 8.1 durchführen

Von Version 7.1 auf Version 8.1 ist ein direktes Upgrade des Servers möglich. Sie müssen Version 7.1 nicht deinstallieren.

Vorbereitende Schritte

Stellen Sie sicher, dass die Installationsmedien für das Basisrelease der Server, für das Sie ein Upgrade durchführen wollen, vorhanden sind. Wenn Sie die Serverkomponenten von DVD installiert haben, stellen Sie sicher, dass die DVD verfügbar ist. Wenn Sie die Serverkomponenten über ein heruntergeladenes Paket installiert haben, stellen Sie sicher, dass die heruntergeladenen Dateien verfügbar sind. Wenn das Upgrade fehlschlägt und das Serverlizenzmodul deinstalliert wird, sind die Installationsmedien für das Basisrelease des Servers für die Neuinstallation der Lizenz erforderlich.

Tipp: Bei Version 8.1 und höher sind DVDs nicht mehr verfügbar.

Vorgehensweise

Führen Sie folgende Tasks aus, um ein Upgrade des Servers auf Version 8.1 durchzuführen:

1. „Planung des Upgrades ” auf Seite 118
2. „Vorbereitung des Systems ” auf Seite 118
3. „Server installieren und Upgrade prüfen” auf Seite 120

Planung des Upgrades

Bevor Sie ein Upgrade des Servers von Version 7.1 auf Version 8.1 durchführen, müssen Sie die relevanten Planungsinformationen lesen, z. B. die Systemvoraussetzungen und die Releaseinformationen. Dann wählen Sie einen geeigneten Zeitpunkt für das Systemupgrade aus, um die Auswirkung auf den Produktionsbetrieb so gering wie möglich zu halten.

Informationen zu diesem Vorgang

In Labortests dauerte der Upgradeprozess für den Server von Version 7.1 auf Version 8.1 14 bis 45 Minuten. Die Dauer in Ihrer Umgebung kann abweichen und ist von Ihrer Hardware und Software sowie der Größe der Serverdatenbank abhängig.

Vorgehensweise

1. Überprüfen Sie die Hardware- und Softwarevoraussetzungen:

   Systemvoraussetzungen für Linux-Systeme

   Aktuelle Informationen zu den Systemvoraussetzungen finden Sie auf der IBM Spectrum Protect-Unterstützungswebsite unter Technote 1243309.
2. Lesen Sie die Releaseinformationen (http://www.ibm.com/support/knowledgecenter/SSEQVQ_8.1.11/srv.common/r_relnotes_srv.html) und die Readme-Dateien für Serverkomponenten, die spezielle Anweisungen und Informationen für Ihr Betriebssystem enthalten.
3. Lesen Sie die Planungsinformationen für die Sicherheitsupdates in „Was Sie vor der Installation oder dem Upgrade des Servers über die Sicherheit wissen sollten” auf Seite 3.
4. Wählen Sie einen geeigneten Zeitpunkt für das Systemupgrade aus, um die Auswirkung auf den Produktionsbetrieb so gering wie möglich zu halten. Die für die Aktualisierung des Systems erforderliche Zeit ist von der Größe der Datenbank und vielen anderen Faktoren abhängig. Wenn Sie den Upgradeprozess starten, können Clients keine Verbindung zum Server herstellen, bis die neue Software installiert ist und alle erforderlichen Lizenzen wieder registriert sind.
5. Wenn Sie ein Upgrade des Servers von Version 7 auf Version 8.1 durchführen, müssen Sie die System-ID und das Kennwort für die IBM Db2-Instanz des IBM Spectrum Protect-Servers kennen. Diese Berechtigungsnachweise sind für ein Upgrade des Systems erforderlich.

Vorbereitung des Systems

Um das System für das Upgrade von Version 7.1 auf Version 8.1 vorzubereiten, müssen Sie Informationen zu jeder IBM Db2-Instanz zusammenstellen. Dann sichern Sie die Serverdatenbank, speichern Sie Schlüsselkonfigurationsdateien, brechen Sie Sitzungen ab und stoppen Sie den Server.

Vorgehensweise

1. Melden Sie sich bei dem Computer an, auf dem der Server installiert ist.

   Stellen Sie sicher, dass Sie mit der Instanzbenutzer-ID angemeldet sind.
2. Rufen Sie eine Liste der Db2-Instanzen ab. Geben Sie den folgenden Systembefehl aus:

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

   Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

   ```
   tsminst1
   ```

   Stellen Sie sicher, dass jede Instanz einem Server entspricht, der auf dem System aktiv ist.
3. Notieren Sie für jede Db2-Instanz den Standarddatenbankpfad, den tatsächlichen Datenbankpfad, den Datenbanknamen, den Aliasnamen der Datenbank und alle Db2-Variablen, die für die Instanz konfiguriert wurden. Bewahren Sie die Aufzeichnung für spätere Referenzzwecke auf. Diese Informationen werden für die Zurückschreibung der Datenbank der Version 7.1 benötigt.
4. Stellen Sie mithilfe der Benutzer-ID mit Administratorberechtigung eine Verbindung zum Server her.
5. Sichern Sie die Datenbank mit dem Befehl **BACKUP DB**.

   Die bevorzugte Methode ist eine Momentaufnahmesicherung, bei der eine Datenbankgesamtsicherung erstellt wird, ohne geplante Datenbanksicherungen zu unterbrechen.

   Sie können eine Momentaufnahmesicherung beispielsweise mit dem folgenden Befehl erstellen:

   ```
   backup db type=dbsnapshot devclass=tapeclass
   ```
6. Geben Sie den folgenden Verwaltungsbefehl aus, um die Einheitenkonfigurationsdaten in einem anderen Verzeichnis zu sichern:

   ```
   backup devconfig filenames=Dateiname
   ```

   Dateiname gibt den Namen der Datei an, in der Einheitenkonfigurationsdaten gespeichert werden sollen.

   Tipp: Diese Datei wird benötigt, wenn die Datenbank der Version 7.1 zurückgeschrieben werden soll.
7. Sichern Sie die Protokolldatei für Datenträger in einem anderen Verzeichnis. Geben Sie den folgenden Verwaltungsbefehl aus:

   ```
   backup volhistory filenames=Dateiname
   ```

   Dateiname gibt den Namen der Datei an, in der Datenträgerhistory-Informationen (Datenträgerprotokolldaten) gespeichert werden sollen.

   Tipp: Diese Datei wird benötigt, wenn die Datenbank der Version 7.1 zurückgeschrieben werden soll.
8. Speichern Sie eine Kopie der Serveroptionsdatei, die normalerweise `dsmserv.opt` heißt. Die Datei befindet sich im Serverinstanzverzeichnis.
9. Verhindern Sie Aktivität auf dem Server durch Inaktivierung neuer Sitzungen. Geben Sie die folgenden Verwaltungsbefehle aus:

   ```
   disable sessions client
   disable sessions server
   ```
10. Überprüfen Sie, ob Sitzungen bestehen, und benachrichtigen Sie die Benutzer, dass der Server gestoppt wird. Geben Sie den folgenden Verwaltungsbefehl aus, um auf bestehende Sitzungen zu überprüfen:

    ```
    query session
    ```
11. Geben Sie den folgenden Verwaltungsbefehl aus, um Sitzungen abzubrechen:

```
cancel session all
```

Dieser Befehl bricht alle Sitzungen außer der aktuellen Sitzung ab.

12. Geben Sie den folgenden Verwaltungsbefehl aus, um den Server zu stoppen:

```
halt
```

13. Stellen Sie sicher, dass der Server heruntergefahren wird und dass keine Prozesse ausgeführt werden.

    Geben Sie den folgenden Befehl aus:

```
ps -ef | grep dsmserv
```

14. Suchen Sie die Datei NODELOCK im Serverinstanzverzeichnis Ihrer Installation und verschieben Sie sie in ein anderes Verzeichnis, in dem Sie Konfigurationsdateien speichern.

    Die Datei NODELOCK enthält die vorherigen Lizenzinformationen für Ihre Installation. Diese Lizenzinformationen werden bei Beendigung des Upgrades ersetzt.

Server installieren und Upgrade prüfen

Sie müssen den Server der Version Version 8.1 installieren, um den Upgradeprozess des Servers auf Version 8.1 abzuschließen. Dann überprüfen Sie, ob das Upgrade erfolgreich war, indem Sie die Serverinstanz starten.

Vorbereitende Schritte

Sie müssen mit der Rootbenutzer-ID am System angemeldet sein.

Das Installationspaket kann von einer IBM Download-Site heruntergeladen werden.

Legen Sie als Systembenutzergrenzwert für die maximale Dateigröße 'unlimited' (unbegrenzt) fest, um sicherzustellen, dass die Dateien ordnungsgemäß heruntergeladen werden können.

1. Führen Sie den folgenden Befehl aus, um den Wert für die maximale Dateigröße abzufragen:

```
ulimit -Hf
```

2. Wenn als Systembenutzergrenzwert für die maximale Dateigröße nicht 'unlimited' (unbegrenzt) angegeben ist, geben Sie 'unlimited' gemäß den Anweisungen in der Dokumentation Ihres Betriebssystems an.

Informationen zu diesem Vorgang

Mithilfe der IBM Spectrum Protect-Installationssoftware können Sie die folgenden Komponenten installieren:

- Server

  Tipp: Die Datenbank (IBM Db2), Global Security Kit (GSKit) und IBM Java Runtime Environment (JRE) werden automatisch installiert, wenn Sie die Serverkomponente auswählen.
- Sprachen des Servers
- Lizenzen
- Einheiten
- IBM Spectrum Protect for SAN
- Operations Center

Vorgehensweise

1. Laden Sie die entsprechende Paketdatei von einer der folgenden Websites herunter:

- Laden Sie das Serverpaket über Passport Advantage oder Fix Central herunter.
- Die neuesten Informationen, Aktualisierungen und Fixes finden Sie im IBM Support Portal.

2. Führen Sie die folgenden Schritte aus:

   a. Überprüfen Sie, ob genug Speicherbereich zum Speichern der Installationsdateien nach dem Extrahieren aus dem Produktpaket vorhanden ist. Informationen zum Speicherbedarf finden Sie im Downloaddokument für Ihr Produkt.

      - IBM Spectrum Protect Technote 588021
      - IBM Spectrum Protect Extended Edition Technote 588023
      - IBM Spectrum Protect for Data Retention Technote 588025

   b. Laden Sie die Paketdatei in ein beliebiges Verzeichnis herunter. Der Pfad darf maximal 128 Zeichen enthalten. Sie müssen die Installationsdateien in ein leeres Verzeichnis extrahieren. Verwenden Sie kein Verzeichnis, das bereits extrahierte Dateien oder andere Dateien enthält.

      Stellen Sie außerdem sicher, dass Sie über die Ausführberechtigung für die Paketdatei verfügen.

   c. Falls erforderlich, führen Sie den folgenden Befehl aus, um die Dateiberechtigungen zu ändern:

      ```
      chmod a+x Paketname.bin
      ```

      Paketname sieht wie in dem folgenden Beispiel aus:

      ```
      8.1.x.000-IBM-SPSRV-Linuxs390x.bin
      8.1.x.000-IBM-SPSRV-Linuxx86_64.bin
      8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
      ```

      In den Beispielen gibt *8.1.x.000* das Release-Level des Produkts an.

   d. Führen Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

      ```
      ./Paketname.bin
      ```

      Die Extraktion nimmt etwas Zeit in Anspruch, weil das Paket groß ist.

3. Installieren Sie die IBM Spectrum Protect-Software mit einer der folgenden Methoden. Installieren Sie die IBM Spectrum Protect-Lizenz während des Installationsprozesses.

   Tipp: Befinden sich mehrere Serverinstanzen auf Ihrem System, installieren Sie die IBM Spectrum Protect-Software nur einmal, um alle Serverinstanzen zu aktualisieren.

   Installationsassistent

   Befolgen Sie die Anweisungen in „IBM Spectrum Protect mit dem Installationsassistenten installieren” auf Seite 84, um den Server mit dem grafisch orientierten Assistenten von IBM Installation Manager zu installieren.

   Stellen Sie sicher, dass Ihr System die Voraussetzungen für die Verwendung des Installationsassistenten erfüllt. Führen Sie anschließend die Installationsschritte aus. Klicken Sie im Fenster von **IBM Installation Manager** auf das Symbol **Aktualisieren** oder **Ändern**.

   Server im Konsolenmodus installieren

   Befolgen Sie die Anweisungen in „IBM Spectrum Protect im Konsolenmodus installieren” auf Seite 85, um den Server im Konsolenmodus zu installieren.

   Lesen Sie die Informationen zur Installation des Servers im Konsolenmodus und führen Sie anschließend die Installationsschritte aus.

   Unbeaufsichtigter Modus

   Befolgen Sie die Anweisungen in „IBM Spectrum Protect im unbeaufsichtigten Modus installieren” auf Seite 85, um den Server im unbeaufsichtigten Modus zu installieren.

Lesen Sie die Informationen zur Installation des Servers im unbeaufsichtigten Modus und führen Sie anschließend die Installationsschritte aus.

Nach der Installation der Software müssen Sie das System nicht rekonfigurieren.

4. Beheben Sie alle Fehler, die während des Installationsprozesses festgestellt werden.

   Wenn Sie den Server mithilfe des Installationsassistenten installiert haben, können Sie Installationsprotokolle mithilfe des Tools IBM Installation Manager anzeigen. Klicken Sie auf **Datei** > **Protokoll anzeigen**. Um Protokolldateien zu erfassen, klicken Sie in IBM Installation Manager auf **Hilfe** > **Daten zur Fehleranalyse exportieren**.

   Wenn Sie den Server im Konsolenmodus oder im unbeaufsichtigten Modus installiert haben, können Sie Fehlerprotokolle im IBM Installation Manager-Protokollverzeichnis anzeigen. Zum Beispiel:

   ```
   /var/ibm/InstallationManager/logs
   ```

5. Rufen Sie das IBM Support Portal auf, um Fixes abzurufen. Klicken Sie auf **Fixes, updates, and drivers** und legen Sie alle gültigen Fixes an.
6. Überprüfen Sie, ob das Upgrade erfolgreich war:
   a) Starten Sie die Serverinstanz.
   b) Überwachen Sie die Nachrichten, die der Server bei seinem Start ausgibt. Achten Sie auf Fehlernachrichten und Warnungen und lösen Sie alle Probleme.
   c) Überprüfen Sie, ob Sie mithilfe des Verwaltungsclients eine Verbindung zum Server herstellen können. Führen Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um eine Verwaltungsclientsitzung zu starten:

      ```
      dsmadmc
      ```

   d) Führen Sie **QUERY**-Befehle aus, um Informationen zum aktualisierten System abzurufen. Führen Sie beispielsweise den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um konsolidierte Informationen zum System abzurufen:

      ```
      query system
      ```

      Führen Sie den folgenden IBM Spectrum Protect-Verwaltungsbefehl aus, um Informationen zur Datenbank abzurufen:

      ```
      query db format=detailed
      ```

7. Registrieren Sie die Lizenzen für die IBM Spectrum Protect-Serverkomponenten, die auf Ihrem System installiert sind. Führen Sie hierfür den Befehl **REGISTER LICENSE** aus:

   ```
   register license file=Installationsverzeichnis/server/bin/Komponentenname.lic
   ```

   Erläuterungen: *Installationsverzeichnis* gibt das Verzeichnis an, in dem Sie die Komponente installiert haben, und *Komponentenname* ist die Abkürzung für die Komponente.

   Wenn Sie den Server beispielsweise im Standardverzeichnis `/opt/tivoli/tsm` installiert haben, registrieren Sie die Lizenz mit dem folgenden Befehl:

   ```
   register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
   ```

   Wenn Sie IBM Spectrum Protect Extended Edition beispielsweise im Verzeichnis `/opt/tivoli/tsm` installiert haben, führen Sie den folgenden Befehl aus:

   ```
   register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
   ```

   Wenn Sie IBM Spectrum Protect for Data Retention beispielsweise im Verzeichnis `/opt/tivoli/tsm` installiert haben, führen Sie den folgenden Befehl aus:

   ```
   register license file=/opt/tivoli/tsm/server/bin/dataret.lic
   ```

Einschränkung:

Sie können den IBM Spectrum Protect-Server nicht zum Registrieren von Lizenzen für die folgenden Produkte verwenden:

- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

Der Befehl **REGISTER LICENSE** ist für diese Lizenzen nicht gültig. Die Lizenzierung für diese Produkte wird von IBM Spectrum Protect-Clients ausgeführt.

8. Bereiten Sie den Server für automatische und manuelle Datenbanksicherungsoperationen vor.

   Anweisungen siehe „Server für Datenbanksicherungsoperationen vorbereiten” auf Seite 108.
9. Optional: Für die Installation eines zusätzlichen Sprachenpakets verwenden Sie die Funktion 'Ändern' von IBM Installation Manager.
10. Optional: Für ein Upgrade auf eine neuere Version eines Sprachenpakets verwenden Sie die Funktion 'Aktualisieren' von IBM Installation Manager.
11. Um die Fehlerbehebung für den Fall späterer Probleme zu erleichtern, stellen Sie sicher, dass genügend Speicherbereich für einen Kernspeicherauszug zugeordnet ist. Weitere Informationen finden Sie in Technote 6357399.

Nächste Schritte

Sie können Kennwörter im LDAP-Verzeichnisserver oder im IBM Spectrum Protect-Server authentifizieren. Im LDAP-Verzeichnisserver authentifizierte Kennwörter können erweiterte Systemsicherheit zur Verfügung stellen.

Server-Upgrade in einer Clusterumgebung durchführen

Sie müssen Vorbereitungs- und Installationstasks ausführen, um ein Upgrade eines Servers in einer Clusterumgebung durchführen zu können. Die Vorgehensweise ist vom Betriebssystem und vom Release abhängig.

Vorgehensweise

Führen Sie die Schritte für Ihr Betriebssystem, Quellenrelease und Zielrelease aus:

Tabelle 22. Prozeduren für ein Upgrade des Servers in einer Clusterumgebung in einem Linux-Betriebssystem

Quellenrelease	Zielrelease	Prozedur
Version 6.3 oder höher	Version 8.1	Upgrade für einen Server durchführen, der mit System Automation for Multiplatforms konfiguriert ist

Upgrade für IBM Spectrum Protect in einer Clusterumgebung durchführen

Um die Vorteile der neuen Features in IBM Spectrum Protect nutzen zu können, können Sie ein Upgrade für den IBM Spectrum Protect-Server durchführen, der unter einem Linux-Betriebssystem in einer Clusterumgebung installiert ist.

Vorgehensweise

Für das Upgrade befolgen Sie die Anweisungen im Abschnitt zum Konfigurieren einer Linux-Umgebung für das Clustering.

Kapitel 6. Referenz: IBM Db2-Befehle für IBM Spectrum Protect-Serverdatenbanken

Verwenden Sie diese Liste als Referenz, wenn der IBM Support Sie anweist, Db2-Befehle auszugeben.

Zweck

Nach der Installation und Konfiguration von IBM Spectrum Protect mithilfe der Assistenten müssen Sie Db2-Befehle nur selten verwenden. Eine begrenzte Gruppe von Db2-Befehlen, die Sie verwenden bzw. zu deren Verwendung Sie aufgefordert werden könnten, ist in der Tabelle aufgelistet.

Diese Liste ist nicht umfassend, es handelt sich lediglich um ergänzende Informationen. Es besteht keine Implikation, dass ein IBM Spectrum Protect-Administrator sie täglich oder regelmäßig verwendet. Beispiele einiger Befehle sind angegeben. Ausgabedaten sind nicht enthalten.

Vollständige Erläuterungen zu den hier beschriebenen Befehlen und zu deren Syntax finden Sie in der Db2-Produktdokumentation.

Tabelle 23. Db2-Befehle

Befehl	Beschreibung	Beispiel
db2icrt	Erstellt Db2-Instanzen im Ausgangsverzeichnis des Instanzeigners. **Tipp:** Der IBM Spectrum Protect-Konfigurationsassistent erstellt die vom Server und von der Datenbank verwendete Instanz. Nach der Installation und Konfiguration eines Servers mithilfe des Konfigurationsassistenten wird der Befehl **db2icrt** in der Regel nicht verwendet. Dieses Dienstprogramm befindet sich im Verzeichnis `DB2DIR/instance`. Hierbei steht `DB2DIR` für das Installationsverzeichnis, in dem die aktuelle Version des Db2-Datenbanksystems installiert ist.	IBM Spectrum Protect-Instanz manuell erstellen (geben Sie den Befehl in einer einzigen Zeile ein): `/opt/tivoli/tsm/db2/instance/db2icrt -a server -u` *`Instanzname Instanzname`*
db2set	Zeigt Db2-Variablen an.	Db2-Variablen auflisten: `db2set`
CATALOG DATABASE	Speichert Informationen zur Speicherposition der Datenbank im Systemdatenbankverzeichnis. Die Datenbank kann sich auf der lokalen Workstation oder auf einem fernen Datenbankpartitionsserver befinden. Der Serverkonfigurationsassistent kümmert sich um jeden Katalog, der zur Verwendung der Serverdatenbank benötigt wird. Führen Sie diesen Befehl nach der Konfiguration und Aktivierung eines Servers nur dann manuell aus, wenn es eine Änderung oder Beschädigung in der Umgebung gibt.	Datenbank katalogisieren: `db2 catalog database tsmdb1`
CONNECT TO DATABASE	Stellt eine Verbindung zu einer angegebenen Datenbank für Befehlszeilenschnittstellenzwecke her.	Eine Verbindung zur IBM Spectrum Protect-Datenbank über eine Db2-Befehlszeilenschnittstelle herstellen: `db2 connect to tsmdb1`

Tabelle 23. Db2-Befehle (Forts.)

Befehl	Beschreibung	Beispiel

GET DATABASE CONFIGURATION	Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück.
	Wichtig: Dieser Befehl und seine Parameter werden direkt von Db2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.
		Die Konfigurationsdaten für einen Datenbankaliasnamen anzeigen:
		`db2 get db cfg for tsmdb1`
		Informationen abrufen, um Einstellungen zu überprüfen (z. B. Datenbankkonfiguration, Protokollmodus und Pflege).
		`db2 get db config for tsmdb1 show detail`

GET DATABASE MANAGER CONFIGURATION	Gibt die Werte einzelner Einträge in einer bestimmten Datenbankkonfigurationsdatei zurück. **Wichtig:** Dieser Befehl und seine Parameter werden direkt von Db2 definiert und verwaltet. Sie sind an dieser Stelle für Informationszwecke aufgelistet, um zu zeigen, wie die vorhandenen Einstellungen abgerufen werden können. Eine Änderung dieser Einstellungen könnte durch IBM Support oder Service-Bulletins wie z. B. APARs oder "Technical Guidance"-Dokumente (Technotes) empfohlen werden. Ändern Sie diese Einstellungen nicht manuell. Nehmen Sie eine Änderung nur nach einer entsprechenden Anweisung von IBM und nur mithilfe von IBM Spectrum Protect-Serverbefehlen oder -Prozeduren vor.	Konfigurationsdaten für den Datenbankmanager abrufen: `db2 get dbm cfg`
GET HEALTH SNAPSHOT	Ruft die Informationen zum Allgemeinzustand für den Datenbankmanager und seine Datenbanken ab. Die zurückgegebenen Informationen stellen eine Momentaufnahme des Status zum Zeitpunkt der Befehlsausgabe dar. IBM Spectrum Protect überwacht den Status der Datenbank mithilfe der Diagnosemomentaufnahme und anderer Mechanismen, die von Db2 bereitgestellt werden. Es kann vorkommen, dass die Diagnosemomentaufnahme oder andere Dokumentation anzeigt, dass sich ein Element bzw. eine Datenbankressource im Alertstatus befindet. In einem solchen Fall müssen entsprechende Schritte zur Behebung der Situation in Betracht gezogen werden. IBM Spectrum Protect überwacht die Bedingung und reagiert entsprechend. Nicht alle deklarierten Alerts der Db2-Datenbank haben Maßnahmen zur Folge.	Einen Bericht über Anzeiger des Db2-Diagnosemonitors abrufen: `db2 get health snapshot for database on tsmdb1`

Tabelle 23. Db2-Befehle (Forts.)

Befehl	Beschreibung	Beispiel

GRANT (Datenbank- berechtigungen)	Erteilt Berechtigungen, die sich auf die gesamte Datenbank beziehen, und keine Zugriffsrechte, die sich auf bestimmte Objekte in der Datenbank beziehen.	Der Benutzer-ID itmuser Zugriffsberechtigung erteilen:
		`db2 GRANT CONNECT ON DATABASE TO USER itmuser`
		`db2 GRANT CREATETAB ON DATABASE TO USER itmuser`

RUNSTATS	Aktualisiert statistische Daten zu den Merkmalen einer Tabelle und der zugeordneten Indizes oder Statistiksichten. Zu diesen Merkmalen gehören die Anzahl der Datensätze, die Anzahl der Seiten und die durchschnittliche Datensatzlänge. Soll eine Tabelle angezeigt werden, verwenden Sie dieses Dienstprogramm nach dem Aktualisieren oder Reorganisieren der Tabelle. Eine Sicht muss für die Optimierung aktiviert sein, damit ihre statistischen Daten für die Optimierung einer Abfrage verwendet werden können. Eine für die Optimierung aktivierte Sicht wird als Statistiksicht bezeichnet. Sie können eine Sicht mit der Db2-Anweisung **ALTER VIEW** für die Optimierung aktivieren. Verwenden Sie das Dienstprogramm **RUNSTATS**, wenn sich Änderungen zugrunde liegender Tabellen auf die von der Sicht zurückgegebenen Zeilen auswirken. **Tipp:** Der Server konfiguriert Db2 so, dass der Befehl **RUNSTATS** nach Bedarf ausgeführt wird.	Statistische Daten für eine einzelne Tabelle aktualisieren. `db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes all`
SET SCHEMA	Ändert den Wert des Sonderregisters **CURRENT SCHEMA** als Vorbereitung für die direkte Ausgabe von SQL-Befehlen über die Db2-Befehlszeilenschnittstelle. **Tipp:** Ein Sonderregister ist ein Speicherbereich, den der Datenbankmanager für einen Anwendungsprozess definiert. In diesem Bereich werden Informationen gespeichert, auf die in SQL-Anweisungen verwiesen werden kann.	Das Schema für IBM Spectrum Protect festlegen: `db2 set schema tsmdb1`
START DATABASE MANAGER	Startet die Hintergrundprozesse der aktuellen Datenbankmanagerinstanz. Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers. **Wichtig:** Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.	Den Datenbankmanager starten: `db2start`

Tabelle 23. Db2-Befehle (Forts.)

Befehl	Beschreibung	Beispiel
STOP DATABASE MANAGER	Stoppt die aktuelle Datenbankmanagerinstanz. Der Datenbankmanager bleibt so lange aktiv, bis er explizit gestoppt wird. Dieser Befehl stoppt die Datenbankmanagerinstanz nicht, wenn Anwendungen mit Datenbanken verbunden sind. Liegen keine Datenbankverbindungen, aber Instanzverbindungen vor, erzwingt der Befehl zunächst das Stoppen der Instanzverbindungen. Dann wird der Datenbankmanager gestoppt. Dieser Befehl inaktiviert außerdem alle ausstehenden Datenbankaktivierungen, bevor der Datenbankmanager gestoppt wird. Dieser Befehl ist auf einem Client nicht gültig. Der Server startet und stoppt die Instanz und die Datenbank bei jedem Start und Stopp des Servers. **Wichtig:** Lassen Sie den Server das Starten und Stoppen der Instanz und der Datenbank steuern, sofern keine anderweitige Anweisung durch IBM Support vorliegt.	Den Datenbankmanager stoppen: `db2 stop dbm`

Kapitel 7. IBM Spectrum Protect deinstallieren

Sie können IBM Spectrum Protect mit den folgenden Methoden deinstallieren. Vor dem Entfernen von IBM Spectrum Protect müssen Sie sicherstellen, dass Ihre Sicherungs- und Archivierungsdaten nicht verloren gehen.

Vorbereitende Schritte

Führen Sie folgende Schritte aus, bevor Sie IBM Spectrum Protect deinstallieren:

- Führen Sie eine Gesamtsicherung der Datenbank aus.
- Speichern Sie eine Kopie der Datenträgerhistory- und Einheitenkonfigurationsdateien.
- Bewahren Sie die Ausgabedatenträger an einem sicheren Ort auf.

Informationen zu diesem Vorgang

Sie können IBM Spectrum Protect mit jeder der folgenden Methoden deinstallieren: grafisch orientierter Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

Nächste Schritte

Installieren Sie die IBM Spectrum Protect-Komponenten erneut.

IBM Spectrum Protect mit einem grafisch orientierten Assistenten deinstallieren

Sie können IBM Spectrum Protect mit dem Installationsassistenten von IBM Installation Manager deinstallieren.

Vorgehensweise

1. Starten Sie Installation Manager.

   In dem Verzeichnis, in dem Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis `eclipse` (z. B. `/opt/IBM/InstallationManager/eclipse`) und geben Sie folgenden Befehl aus:

   ```
   ./IBMIM
   ```

2. Klicken Sie auf **Deinstallieren**.
3. Wählen Sie **IBM Spectrum Protect-Server** aus und klicken Sie auf **Weiter**.
4. Klicken Sie auf **Deinstallieren**.
5. Klicken Sie auf **Fertigstellen**.

IBM Spectrum Protect im Konsolenmodus deinstallieren

Zum Deinstallieren von IBM Spectrum Protect mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.

Vorgehensweise

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:

   `eclipse/tools`

Beispiel:

```
/opt/IBM/InstallationManager/eclipse/tools
```

2. Im Verzeichnis `tools` geben Sie den folgenden Befehl aus:

```
./imcl -c
```

3. Für die Deinstallation geben Sie 5 ein.
4. Wählen Sie die Deinstallation aus der IBM Spectrum Protect-Paketgruppe aus.
5. Geben Sie N für 'Next' (Weiter) ein.
6. Wählen Sie die Deinstallation des IBM Spectrum Protect-Serverpakets aus.
7. Geben Sie N für 'Next' (Weiter) ein.
8. Geben Sie U für 'Uninstall' (Deinstallieren) ein.
9. Geben Sie F für 'Finish' (Fertigstellen) ein.

IBM Spectrum Protect im unbeaufsichtigten Modus deinstallieren

Zum Deinstallieren von IBM Spectrum Protect im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.

Vorbereitende Schritte

Sie können die Dateneingabe für eine unbeaufsichtigte Deinstallation der IBM Spectrum Protect-Serverkomponenten mithilfe einer Antwortdatei bereitstellen. IBM Spectrum Protect enthält eine Musterantwortdatei, `uninstall_response_sample.xml`, im Verzeichnis `input`, in dem das Installationspaket extrahiert wird. Diese Datei enthält Standardwerte, durch die Sie unnötige Warnungen vermeiden können.

Wenn Sie alle IBM Spectrum Protect-Komponenten deinstallieren wollen, lassen Sie die Einstellung `modify="false"` für jede Komponente in der Antwortdatei unverändert. Wenn Sie eine Komponente nicht deinstallieren wollen, geben Sie den Wert `modify="true"` an.

Wenn Sie die Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

Vorgehensweise

1. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das folgende Unterverzeichnis:

   ```
   eclipse/tools
   ```

   Beispiel:

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

2. Im Verzeichnis `tools` geben Sie den folgenden Befehl aus, wobei *Antwortdatei* den Pfad der Antwortdatei einschließlich des Dateinamens angibt:

   ```
   ./imcl -input Antwortdatei -silent
   ```

   Der folgende Befehl ist ein Beispiel:

   ```
   ./imcl -input /tmp/input/uninstall_response.xml -silent
   ```

IBM Spectrum Protect deinstallieren und erneut installieren

Wenn Sie IBM Spectrum Protect nicht mit dem Assistenten, sondern manuell erneut installieren wollen, müssen Sie einige Maßnahmen ergreifen, um Ihre Serverinstanznamen und Datenbankverzeichnisse zu bewahren. Während einer Deinstallation werden alle bereits definierten Serverinstanzen entfernt, die Datenbankkataloge für diese Instanzen sind jedoch noch vorhanden.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um IBM Spectrum Protect manuell zu deinstallieren und erneut zu installieren:

1. Erstellen Sie eine Liste Ihrer aktuellen Serverinstanzen, bevor Sie mit der Deinstallation beginnen. Führen Sie den folgenden Befehl aus:

   ```
   /opt/tivoli/tsm/db2/instance/db2ilist
   ```

2. Führen Sie die folgenden Befehle für jede Serverinstanz aus:

   ```
   db2 attach to Instanzname
   db2 get dbm cfg show detail
   db2 detach
   ```

   Notieren Sie den Datenbankpfad für jede Instanz.

3. Deinstallieren Sie IBM Spectrum Protect.
4. Wenn Sie eine beliebige unterstützte Version von IBM Spectrum Protect deinstallieren (einschließlich Fixpack), wird eine Instanzdatei erstellt. Die Instanzdatei wird erstellt, um die Reinstallation von IBM Spectrum Protect zu erleichtern. Überprüfen Sie diese Datei und verwenden Sie die Informationen, wenn Sie bei der Reinstallation zur Eingabe der Berechtigungsnachweise der Instanz aufgefordert werden. Bei der unbeaufsichtigten Installation geben Sie diese Berechtigungsnachweise mit der Variablen `INSTANCE_CRED` an.

   Sie finden die Instanzdatei an der folgenden Position:

   `/etc/tivoli/tsm/instanceList.obj`

5. Installieren Sie IBM Spectrum Protect erneut.

   Ist die Datei `instanceList.obj` nicht vorhanden, müssen Sie Ihre Serverinstanzen wie folgt erneut erstellen:

   a. Erstellen Sie Ihre Serverinstanzen erneut.

      Tipp: Der Installationsassistent konfiguriert die Serverinstanzen, Sie müssen jedoch überprüfen, ob sie vorhanden sind. Wenn sie nicht vorhanden sind, müssen Sie sie manuell konfigurieren.

   b. Katalogisieren Sie die Datenbank. Melden Sie sich bei jeder Serverinstanz nacheinander als Instanzbenutzer an und geben Sie folgende Befehle aus:

      ```
      db2 catalog database tsmdb1
      db2 attach to Instanzname
      db2 update dbm cfg using dftdbpath Instanzverzeichnis
      db2 detach
      ```

   c. Überprüfen Sie, ob die Serverinstanz erfolgreich erstellt wurde. Geben Sie den folgenden Befehl aus:

      ```
      /opt/tivoli/tsm/db2/instance/db2ilist
      ```

   d. Überprüfen Sie, ob IBM Spectrum Protect die Serverinstanz erkennt, indem Sie Ihre Verzeichnisse auflisten. Ihr Ausgangsverzeichnis wird angezeigt, wenn Sie es nicht geändert haben. Ihr Instanzverzeichnis wird angezeigt, wenn Sie den Konfigurationsassistenten verwendet haben. Geben Sie den folgenden Befehl aus:

      ```
      db2 list database directory
      ```

      Wenn Sie TSMDB1 in der Liste finden, können Sie den Server starten.

IBM Installation Manager deinstallieren

Sie können IBM Installation Manager deinstallieren, wenn keine Produkte mehr vorhanden sind, die mit IBM Installation Manager installiert wurden.

Vorbereitende Schritte

Bevor Sie IBM Installation Manager deinstallieren, müssen Sie sicherstellen, dass alle mit IBM Installation Manager installierten Pakete deinstalliert sind. Schließen Sie IBM Installation Manager, bevor Sie den Deinstallationsprozess starten.

Geben Sie den folgenden Befehl in eine Befehlszeile ein, um installierte Pakete anzuzeigen:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

Prozedur

Gehen Sie wie folgt vor, um IBM Installation Manager zu deinstallieren:

- 1. Öffnen Sie eine Befehlszeile und wechseln Sie in das Verzeichnis `/var/ibm/InstallationManager/uninstall`.
  2. Geben Sie den folgenden Befehl aus:

     ```
     ./uninstall
     ```

     Einschränkung: Sie müssen mit der Benutzer-ID `root` am System angemeldet sein.

Teil 2. Operations Center installieren und Operations Center-Upgrade durchführen

Das IBM Spectrum Protect Operations Center ist die webbasierte Schnittstelle für die Verwaltung Ihrer Speicherumgebung.

Vorbereitende Schritte

Lesen Sie die folgenden Informationen, bevor Sie das Operations Center installieren und konfigurieren:

- Systemvoraussetzungen für das Operations Center
  - Voraussetzungen für den Computer des Operations Center
  - Voraussetzungen für Hub- und Peripherieserver
  - Betriebssystemvoraussetzungen
  - Voraussetzungen für den Web-Browser
  - Voraussetzungen für die Sprache
  - Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices
- Administrator-IDs, die für das Operations Center erforderlich sind
- IBM Installation Manager
- Prüfliste für die Installation
- Operations Center-Installationspaket abrufen

Informationen zu diesem Vorgang

In Tabelle 24 auf Seite 133 sind die Methoden für die Installation oder Deinstallation des Operations Center aufgelistet. Außerdem ist angegeben, wo Sie die zugehörigen Anweisungen finden.

Informationen zum Upgrade des Operations Center finden Sie in Upgrade des Operations Center.

Tabelle 24. Methoden für die Installation oder Deinstallation des Operations Center

Methode	Anweisungen
Grafisch orientierter Assistent	• Operations Center mit einem grafisch orientierten Assistenten installieren • Operations Center mit einem grafisch orientierten Assistenten deinstallieren
Konsolenmodus	• Operations Center im Konsolenmodus installieren • Operations Center im Konsolenmodus deinstallieren
Unbeaufsichtigter Modus	• Operations Center im unbeaufsichtigten Modus installieren • „Operations Center im unbeaufsichtigten Modus deinstallieren” auf Seite 204

Kapitel 8. Installation des Operations Center planen

Vor der Installation des Operations Center müssen Sie die Systemvoraussetzungen, die Administrator-IDs, die das Operations Center benötigt, und die im Installationsprogramm anzugebenden Informationen kennen.

Informationen zu diesem Vorgang

Mithilfe des Operations Center können Sie die folgenden Hauptaspekte der Speicherumgebung verwalten:

- IBM Spectrum Protect-Server und -Clients
- Services wie Sichern und Zurückschreiben, Archivieren und Abrufen sowie Umlagern und Zurückrufen
- Speicherpool und Speichereinheiten

Das Operations Center verfügt über folgende Funktionen:

Benutzerschnittstelle für mehrere Server
Sie können mit dem Operations Center mindestens einen IBM Spectrum Protect-Server verwalten.

In einer Umgebung mit mehreren Servern können Sie einen Server als *Hub-Server* und die übrigen Server als *Peripherieserver* festlegen. Der Hub-Server kann Alerts und Statusinformationen von den Peripherieservern empfangen und in einer konsolidierten Sicht im Operations Center anzeigen.

Alertüberwachung

Ein *Alert* ist eine Benachrichtigung über ein relevantes Problem auf dem Server und wird durch eine Servernachricht ausgelöst. Sie können definieren, welche Nachrichten Alerts auslösen, und nur diese Nachrichten werden als Alerts in der Operations Center oder in einer E-Mail aufgelistet.

Diese Alertüberwachung kann Ihnen beim Erkennen und Verfolgen relevanter Probleme auf dem Server helfen.

Komfortable Befehlszeilenschnittstelle
Das Operations Center verfügt über eine Befehlszeilenschnittstelle für erweiterte Funktionen und Konfiguration.

Systemvoraussetzungen für das Operations Center

Stellen Sie vor der Installation des Operations Center sicher, dass Ihr System die Mindestvoraussetzungen erfüllt.

Mithilfe des Operations Center System Requirements Calculator können Sie die Systemvoraussetzungen für die Ausführung des Operations Center sowie der vom Operations Center überwachten Hub- und Peripherieserver schätzen.

Während der Installation überprüfte Voraussetzungen

Tabelle 25 auf Seite 135 enthält eine Auflistung der Voraussetzungen, die während der Installation überprüft werden, und Verweise auf weitere Informationen zu diesen Voraussetzungen.

Tabelle 25. Während der Installation überprüfte Voraussetzungen

Voraussetzungen	Details
Mindestspeicherbedarf	„Voraussetzungen für den Computer des Operations Center” auf Seite 136
Betriebssystemvoraussetzungen	„Betriebssystemvoraussetzungen” auf Seite 139
Hostnamen des Computers, auf dem das Operations Center installiert werden soll	„Prüfliste für die Installation” auf Seite 144

Tabelle 25. Während der Installation überprüfte Voraussetzungen (Forts.)	
Voraussetzungen	**Details**
Voraussetzungen für das Operations Center-Installationsverzeichnis	„Prüfliste für die Installation” auf Seite 144

Voraussetzungen für den Computer des Operations Center

Sie können das Operations Center auf einem Computer installieren, auf dem auch der IBM Spectrum Protect-Server ausgeführt wird, oder auf einem andere Computer. Wenn Sie das Operations Center zusammen mit einem Server auf demselben Computer installieren, muss dieser Computer die Systemvoraussetzungen für das Operations Center und für den Server erfüllen.

Ressourcenanforderungen

Die folgenden Ressourcen sind für die Ausführung des Operations Center erforderlich:

- Ein Prozessorkern
- 4 GB Speicher
- 1 GB Plattenspeicherplatz

Für den Hub-Server und die Peripherieserver, die vom Operations Center überwacht werden, sind zusätzliche Ressourcen erforderlich (siehe „Voraussetzungen für Hub- und Peripherieserver” auf Seite 136).

Voraussetzungen für Hub- und Peripherieserver

Wenn Sie das Operations Center zum ersten Mal öffnen, müssen Sie das Operations Center einem einzelnen IBM Spectrum Protect-Server zuordnen, der als *Hub-Server* festgelegt ist. In einer Umgebung mit mehreren Servern können Sie die anderen Server, die als *Peripherieserver* bezeichnet werden, mit dem Hub-Server verbinden.

Die Peripherieserver senden Alerts und Statusinformationen an den Hub-Server. Das Operations Center zeigt eine konsolidierte Sicht der Alerts und Statusinformationen für den Hub-Server und alle Peripherieserver an.

Wird nur ein einziger Server vom Operations Center überwacht, wird dieser Server als Hub-Server bezeichnet, obwohl keine Peripherieserver mit ihm verbunden sind.

In Tabelle 26 auf Seite 137 ist die Version des IBM Spectrum Protect-Servers aufgeführt, die auf dem Hub-Server und auf jedem vom Operations Center verwalteten Peripherieserver installiert sein muss.

Tabelle 26. Voraussetzungen bezüglich der IBM Spectrum Protect-Serverversion für Hub- und Peripherieserver

Operations Center	Version auf dem Hub-Server	Version auf jedem Peripherieserver
Version 8.1.12	Version 8.1.12	Version 8.1.10 oder höher ========== oder Version 7.1.10 oder ein höheres Release der Version 7 **Einschränkungen:** • Für Server mit einer Version vor Version 8.1.12 sind einige Operations Center-Funktionen nicht verfügbar. • Ein Peripherieserver kann keine Version verwenden, die höher als die Version auf dem Hub-Server ist.

Informationen zu Kompatibilitätsanforderungen für Hub- und Peripherieserver bei anderen Versionen des Operations Center finden Sie in Technote 496593.

Anzahl Peripherieserver, die ein Hub-Server unterstützen kann

Die Anzahl der Peripherieserver, die ein Hub-Server unterstützen kann, ist von der Konfiguration und von der Version von IBM Spectrum Protect auf jedem Peripherieserver abhängig. Eine allgemeine Richtlinie ist jedoch, dass ein Hub-Server auf einem separaten System (z. B. eine VM) Dutzende Peripherieserver der Version 7.1 oder höher unterstützen kann.

Tipps für das Entwerfen der Hub- und Peripherieserverkonfiguration

Berücksichtigen Sie beim Entwurf der Hub- und Peripherieserverkonfiguration insbesondere die Ressourcenanforderungen für die Statusüberwachung. Überlegen Sie außerdem, wie Sie Hub- und Peripherieserver gruppieren und ob Sie mehrere Hub-Server verwenden wollen.

Mithilfe des Operations Center System Requirements Calculator können Sie die Systemvoraussetzungen für die Ausführung des Operations Center sowie der vom Operations Center überwachten Hub- und Peripherieserver schätzen.

Primäre leistungsrelevante Faktoren

Die folgenden Faktoren haben den größten Einfluss auf die Leistung des Operations Center:

- Der Prozessor und Speicher auf dem Computer, auf dem das Operations Center installiert ist.
- Die Systemressourcen der Hub- und Peripherieserver, einschließlich des für die Hub-Serverdatenbank verwendeten Plattensystems.
- Die Anzahl der Clientknoten und Dateibereiche für virtuelle Maschinen, die von den Hub- und Peripherieservern verwaltet werden.
- Die Aktualisierungshäufigkeit der Daten im Operations Center.

Hub- und Peripherieserver gruppieren

Erwägen Sie die Gruppierung von Hub- und Peripherieservern nach Standort. Durch die Verwaltung der Server in demselben Rechenzentrum können beispielsweise Probleme vermieden werden, die durch Fire-

walls oder unzulängliche Netzbandbreite zwischen verschiedenen Standorten verursacht werden. Bei Bedarf können Sie die Server anhand der folgenden Merkmale weiter unterteilen:

- Administrator, der die Server verwaltet
- Organisationsentität, die die Server finanziert
- Serverbetriebssystem
- Sprache, mit der die Server ausgeführt werden.

  Tipp: Werden Hub- und Peripherieserver nicht mit derselben Sprache ausgeführt, könnte fehlerhafter Text im Operations Center angezeigt werden.

Hub- und Peripherieserver in einer unternehmensweiten Konfiguration gruppieren

In einer unternehmensweiten Konfiguration wird ein IBM Spectrum Protect-Servernetz als Gruppe verwaltet. Im *Konfigurationsmanager* vorgenommene Änderungen können automatisch an mindestens einen *verwalteten Server* im Netz verteilt werden.

Normalerweise registriert und verwaltet das Operations Center eine dedizierte Administrator-ID auf den Hub- und Peripherieservern. Dieser *Überwachungsadministrator* muss auf allen Servern immer dasselbe Kennwort haben.

Wenn Sie eine unternehmensweite Konfiguration verwenden, können Sie den Prozess, durch den die Administratorberechtigungsnachweise auf Peripherieservern synchronisiert werden, verbessern. Gehen Sie wie folgt vor, um die Leistung und Effizienz bei der Verwaltung der Überwachungsadministrator-ID zu verbessern:

1. Legen Sie den Konfigurationsmanagerserver als Hub-Server des Operations Center fest. Während der Hub-Server-Konfiguration wird die Überwachungsadministrator-ID 'IBM-OC-*Hub-Server-Name*' registriert.
2. Auf dem Hub-Server fügen Sie die Überwachungsadministrator-ID einem neuen oder vorhandenen Profil für die unternehmensweite Konfiguration hinzu. Geben Sie den Befehl NOTIFY SUBSCRIBERS aus, um das Profil an die verwalteten Server zu verteilen.
3. Fügen Sie mindestens einen der verwalteten Server als Peripherieserver des Operations Center hinzu.

Das Operations Center erkennt diese Konfiguration und gestattet dem Konfigurationsmanager, die Überwachungsadministrator-ID auf den Peripherienservern zu verteilen und zu aktualisieren.

Verwendung mehrerer Hub-Server

Sind mehr als 10 bis 20 Peripherieserver der Version 6.3.4 vorhanden oder muss die Umgebung aufgrund von Ressourceneinschränkungen partitioniert werden, können Sie mehrere Hub-Server konfigurieren und jeden Hub-Server mit einer Untergruppe der Peripherieserver verbinden.

Einschränkungen:

- Derselbe Server kann nicht gleichzeitig Hub-Server und Peripherieserver sein.
- Jeder Peripherieserver kann nur einem einzigen Hub-Server zugeordnet sein.
- Für jeden Hub-Server ist eine separate Operations Center-Instanz mit einer separaten Webadresse erforderlich.

Tipps für die Auswahl eines Hub-Servers

Als Hub-Server müssen Sie einen Server auswählen, der über angemessene Ressourcen verfügt und sich an einem Standort befindet, der minimale Umlauflatenzzeit im Netz gewährleistet.

Achtung: Verwenden Sie nicht einen einzigen Server als Hub-Server für mehrere Operations Center.

Treffen Sie Ihre Entscheidung darüber, welcher Server als Hub-Server festgelegt werden soll, anhand der folgenden Richtlinien:

Wählen Sie einen Server mit geringer Auslastung
Sie sollten einen Server mit einer geringen Auslastung für Operationen wie z. B. Clientsicherung und -archivierung auswählen. Ein Server mit geringer Auslastung ist auch eine gute Wahl als Hostsystem für das Operations Center.

Stellen Sie sicher, dass der Server über die Ressourcen zur Bearbeitung sowohl seiner normalen Serverauslastung als auch der geschätzten Auslastung für seine Rolle als Hub-Server verfügt.

Positionieren Sie den Server so, dass minimale Umlauflatenzzeit im Netz entsteht
Positionieren Sie den Hub-Server so, dass die Netzverbindung zwischen dem Hub-Server und den Peripherieservern eine Umlauflatenzzeit von maximal 5 ms aufweist. Diese Latenzzeit kann normalerweise erreicht werden, wenn sich die Server in demselben lokalen Netz (LAN) befinden.

Netze, die schlecht eingestellt sind, von anderen Anwendungen stark genutzt werden oder eine Umlauflatenzzeit von sehr viel mehr als 5 ms haben, können die Kommunikation zwischen dem Hub-Server und den Peripherieservern verschlechtern. Umlauflatenzzeiten von 50 ms oder mehr können z. B. Überschreitungen des Kommunikationszeitlimits bewirken, die eine Trennung oder Wiederherstellung der Peripherieserververbindung zum Operations Center verursachen. Derartig lange Latenzzeiten können bei der Kommunikation im Weitverkehrsnetz (WAN) auftreten.

Wenn der Abstand zwischen den Peripherieservern und dem Hub-Server sehr groß ist und häufige Trennungen der Peripherieserververbindung im Operations Center auftreten, können Sie den Wert der Option **ADMINCOMMTIMEOUT** auf jedem Server erhöhen, um das Problem zu verkleinern.

Stellen Sie sicher, dass der Hub-Server die Ressourcenanforderungen für die Statusüberwachung erfüllt
Für die Statusüberwachung werden zusätzliche Ressourcen auf jedem Server benötigt, auf dem sie aktiviert ist. Der Ressourcenbedarf ist hauptsächlich von der Anzahl Clients abhängig, die von den Hub- und Peripherieservern verwaltet werden. Auf einem Hub-Server mit einem Peripherieserver der Version 7.1 oder höher werden weniger Ressourcen verwendet als auf einem Hub-Server mit einem Peripherieserver der Version 6.3.4.

Stellen Sie sicher, dass der Hub-Server die Ressourcenanforderungen bezüglich der Prozessorauslastung, des Datenbankbereichs, des Speicherbereichs für das Archivprotokoll und der IOPS-Kapazität erfüllt (IOPS = E/A-Operationen pro Sekunde).

Ein Hub-Server mit hoher IOPS-Kapazität kann ein hohes Volumen eingehender Statusdaten von Peripherieservern bearbeiten. Die Erfüllung dieser Kapazitätsanforderung kann durch die Verwendung der folgenden Speichereinheiten für die Hub-Server-Datenbank erleichtert werden:

- Ein Solid-State-Laufwerk (SSD) auf Unternehmensebene
- Eine externe SAN-Plattenspeichereinheit mit mehreren Datenträgern oder mehreren Spindeln unter jedem Datenträger

In einer Umgebung mit weniger als 1000 Clients sollten Sie das Einrichten einer Basiskapazität von 1000 E/A-Operationen pro Sekunde für die Hub-Serverdatenbank in Betracht ziehen, wenn der Hub-Server Peripherieserver verwaltet.

Stellen Sie fest, ob in Ihrer Umgebung mehrere Hub-Server erforderlich sind
Wenn eine aus einem Hub-Server und Peripherieservern bestehende Gruppe mehr als 10.000 bis 20.000 Clientknoten und Dateibereiche für virtuelle Maschinen verwaltet, könnte der Ressourcenbedarf die verfügbaren Ressourcen des Hub-Servers übersteigen, insbesondere, wenn es sich bei den Peripherieservern um Server der Version 6.3.4 handelt. In diesem Fall sollten Sie einen zweiten Server als Hub-Server angeben und zum Lastausgleich Peripherieserver zum neuen Hub-Server versetzen.

Betriebssystemvoraussetzungen

Das Operations Center ist für AIX-, Linux- und Windows-Systeme verfügbar.

Sie können das Operations Center auf den folgenden Systemen ausführen.

Falls nicht anders angegeben, ist die Operations Center-Unterstützung für AIX- und Linux-Systeme auf Big Endian-Versionen beschränkt.

- Linux on x86_64-Systeme:
  - Red Hat® Enterprise Linux 8.1 oder höher
  - Red Hat Enterprise Linux 7.6 oder höher
  - SUSE Linux Enterprise Server 15, Service Pack 1 oder höher
  - SUSE Linux Enterprise Server 12, Service Pack 4 oder höher
- Linux on System z-Systeme (s390x 64-Bit-Architektur):
  - Red Hat Enterprise Linux 8.1 oder höher
  - Red Hat Enterprise Linux 7.6 oder höher
  - SUSE Linux Enterprise Server 15, Service Pack 1 oder höher
  - SUSE Linux Enterprise Server 12, Service Pack 4 oder höher
- Linux on Power Systems-Systeme (Little Endian):
  - Red Hat Enterprise Linux 8.1 oder höher
  - Red Hat Enterprise Linux 7.6 oder höher mit PPC64LE-Architektur
  - SUSE Linux Enterprise Server 15, Service Pack 1 oder höher
  - SUSE Linux Enterprise Server 12, Service Pack 4 oder höher

Aktuelle Informationen zu den Anforderungen finden Sie unter Software and Hardware Requirements.

Voraussetzungen für den Web-Browser

Das Operations Center kann in Apple-, Google-, Microsoft- und Mozilla-Web-Browsern ausgeführt werden.

Stellen Sie für eine optimale Anzeige des Operations Center im Web-Browser sicher, dass die Bildschirmauflösung für das System mindestens auf 1024 x 768 Pixel gesetzt ist.

Verwenden Sie einen Web-Browser mit guter JavaScript-Leistung und aktivieren Sie Browser-Caching, um eine optimale Leistung zu erzielen.

Das Operations Center kann in den folgenden Web-Browsern ausgeführt werden:

- Apple Safari auf dem iPad

  Einschränkung: Wird Apple Safari unter iOS 8.x oder iOS 9.x ausgeführt, können Sie ein selbst signiertes Zertifikat für die sichere Kommunikation mit dem Operations Center nur mit zusätzlicher Konfiguration des Zertifikats verwenden. Verwenden Sie ein Zertifikat einer Zertifizierungsstelle (CA-Zertifikat) oder konfigurieren Sie das selbst signierte Zertifikat nach Bedarf. Anweisungen finden Sie im technischen Hinweis (Technote) http://www.ibm.com/support/docview.wss?uid=swg21963153.
- Google Chrome 54 oder höher
- Microsoft Internet Explorer 11 oder höher
- Mozilla Firefox ESR 45 oder Version 48 oder höher

Die Kommunikation zwischen dem Operations Center und dem Web-Browser muss mit dem TLS 1.2-Protokoll (TLS = Transport Layer Security) geschützt werden. Der Web-Browser muss TLS 1.2 unterstützen und TLS 1.2 muss aktiviert sein. Der Web-Browser zeigt einen SSL-Fehler an, wenn diese Voraussetzungen nicht erfüllt sind.

Aktuelle Informationen zu den Anforderungen finden Sie unter Software and Hardware Requirements.

Voraussetzungen für die Sprache

Standardmäßig verwendet das Operations Center dieselbe Sprache wie der Web-Browser. Beim Installationsprozess wird jedoch die Sprache des Betriebssystems verwendet. Überprüfen Sie, ob für den Web-Browser und das Betriebssystem die erforderliche Sprache definiert ist.

Tabelle 27. Operations Center-Sprachwerte, die Sie auf Linux-Systemen verwenden können	
Sprache	**Wert für die Sprachoption**
Chinesisch, vereinfacht	zh_CN
Chinesisch, vereinfacht (GBK)	zh_CN.gb18030
Chinesisch, vereinfacht (UTF-8)	zh_CN.utf8
Chinesisch, traditionell (Big5)	Zh_TW
Chinesisch, traditionell (euc_tw)	zh_TW
Chinesisch, traditionell (UTF-8)	zh_TW.utf8
Englisch, Vereinigte Staaten	en_US
Englisch (UTF-8)	en_US.utf8
Französisch	fr_FR
Französisch (UTF-8)	fr_FR.utf8
Deutsch	de_DE
Deutsch (UTF-8)	de_DE.utf8
Italienisch	it_IT
Italienisch (UTF-8)	it_IT.utf8
Japanisch (EUC)	ja_JP
Japanisch (UTF-8)	ja_JP.utf8
Koreanisch	ko_KR
Koreanisch (UTF-8)	ko_KR.utf8
Portugiesisch, Brasilianisches	pt_BR
Portugiesisch, Brasilianisches (UTF-8)	pt_BR.utf8
Russisch	ru_RU
Russisch (UTF-8)	ru_RU.utf8
Spanisch	es_ES
Spanisch (UTF-8)	es_ES.utf8

Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices

IBM Spectrum Protect-Clientverwaltungsservices ist eine Komponente, die Sie auf Clients für Sichern/Archivieren installieren, um Diagnoseinformationen (z. B. Clientprotokolldateien) zu erfassen. Bevor Sie den Clientverwaltungsservice auf Ihrem System installieren, müssen Sie die Voraussetzungen und Einschränkungen kennen.

In der Dokumentation für den Clientverwaltungsservice ist *Clientsystem* das System, in dem der Client für Sichern/Archivieren installiert ist.

Diagnoseinformationen können nur von Linux- und Windows-Clients erfasst werden. Administratoren können jedoch die Diagnoseinformationen unter AIX, Linux oder Windows im Operations Center anzeigen.

Tipp: Stellen Sie vor der Installation des Clientverwaltungsservice sicher, dass zwischen dem Client für Sichern/Archivieren und dem Server eine Verbindung besteht. Die vom Client verwendete Server-Trust-

store-Datei erhält das SSL-Zertifikat erst, wenn das Clientsystem mit dem Server verbunden ist (SSL = Secure Sockets Layer).

Voraussetzungen für den Clientverwaltungsservice

Lesen Sie die folgenden Informationen zu den Voraussetzungen, bevor Sie den Clientverwaltungsservice installieren:

- Für einen Fernzugriff auf den Client benötigt der Operations Center-Administrator Systemberechtigung oder eine der folgenden Clientberechtigungsstufen:
  - Maßnahmenberechtigung
  - Clienteignerberechtigung
  - Clientknotenzugriffsberechtigung
- Stellen Sie sicher, dass das Clientsystem die folgenden Voraussetzungen erfüllt:
  - Der Clientverwaltungsservice kann nur in Clientsystemen installiert werden, die mit Linux- oder Windows-Betriebssystemen ausgeführt werden:
    - Linux x86-64-Bit-Betriebssysteme, die für den Client für Sichern/Archivieren unterstützt werden
    - Windows-32-Bit- und -64-Bit-Betriebssysteme, die für den Client für Sichern/Archivieren unterstützt werden
  - Für die Datenübertragung zwischen dem Clientverwaltungsservice und dem Operations Center muss Transport Layer Security (TLS) Version 1.2 oder höher installiert sein. Es steht Basisauthentifizierung zur Verfügung und Daten sowie Authentifizierungsinformationen werden über den SSL-Kanal verschlüsselt. TLS wird bei der Installation des Clientverwaltungsservice automatisch zusammen mit den erforderlichen SSL-Zertifikaten installiert.

    Ab IBM Spectrum Protect Version 8.1.11 ist das TLS 1.3-Protokoll für die sichere Kommunikation zwischen Servern, Clients und Speicheragenten standardmäßig aktiviert. Damit TLS 1.3 verwendet werden kann, müssen beide Teilnehmer einer Kommunikationssitzung TLS 1.3 verwenden. Wenn einer der Teilnehmer TLS 1.2 verwendet, verwenden standardmäßig beide Teilnehmer TLS 1.2.
- Auf Linux-Clientsystemen benötigen Sie Rootberechtigung für die Installation des Clientverwaltungsservice.
- Bei Clientsystemen, die mehrere Clientknoten haben können, z. B. Linux-Clientsysteme, muss jeder Knotenname im Clientsystem eindeutig sein.

  Tipp: Nach der Installation des Clientverwaltungsservice müssen Sie ihn nicht erneut installieren, weil der Service mehrere Clientoptionsdateien erkennen kann.

Einschränkungen des Clientverwaltungsservice

Der Clientverwaltungsservice stellt Basisservices für die Erfassung von Diagnoseinformationen aus den Clients für Sichern/Archivieren bereit. Für den Clientverwaltungsservice bestehen die folgenden Einschränkungen:

- Sie können den Clientverwaltungsservice nur auf Systemen mit Clients für Sichern/Archivieren installieren, einschließlich Clients für Sichern/Archivieren, die auf Knoten mit Einheiten zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware installiert sind.
- Sie können den Clientverwaltungsservice nicht auf anderen IBM Spectrum Protect-Clientkomponenten oder -Produkten installieren, die keine Clients für Sichern/Archivieren aufweisen.
- Wenn die Clients für Sichern/Archivieren durch eine Firewall geschützt sind, müssen Sie sicherstellen, dass das Operations Center durch die Firewall mithilfe des konfigurierten Anschlusses für den Clientverwaltungsservice eine Verbindung zu den Clients für Sichern/Archivieren herstellen kann. Der Standardanschluss ist 9028, der jedoch geändert werden kann.
- Der Clientverwaltungsservice überprüft alle Clientprotokolldateien auf Einträge für den vorhergehenden Zeitraum von 72 Stunden.

- Die Diagnoseseite im Operations Center enthält Basisinformationen zur Fehlerbehebung für Clients für Sichern/Archivieren. Bei einigen Sicherungsproblemen müssen Sie jedoch u. U. auf das Clientsystem zugreifen und weitere Diagnoseinformationen abrufen.
- Wenn die Clientfehlerprotokolldateien und die Planungsprotokolldateien in einem Clientsystem zusammen eine Größe von mehr als 500 MB haben, können beim Senden von Protokollsätzen an das Operations Center Verzögerungen auftreten. Sie können die Größe der Protokolldateien steuern, indem Sie eine Bereinigung oder einen Umlauf von Protokolldateien durch Angabe der Clientoption **errorlogretention** bzw. **errorlogmax** ermöglichen.
- Wenn Sie denselben Clientknotennamen verwenden, um eine Verbindung zu mehreren IBM Spectrum Protect-Servern herzustellen, die auf derselben Server-Hardware installiert sind, können Sie Protokolldateien für nur einen der Clientknoten anzeigen.

Informationen zu möglichen Aktualisierungen des Clientverwaltungsservice finden Sie in Technote 534165.

Zugehörige Tasks

„Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen" auf Seite 181
Der Clientverwaltungsservice erfasst Diagnoseinformationen über Clients für Sichern/Archivieren und stellt diese Informationen dem Operations Center für Basisüberwachungsfunktionen zur Verfügung.

Administrator-IDs, die für das Operations Center erforderlich sind

Ein Administrator muss für die Anmeldung beim Operations Center eine gültige ID und ein gültiges Kennwort auf dem Hub-Server haben. Eine Administrator-ID wird auch dem Operations Center zugeordnet, damit das Operations Center Server überwachen kann.

Für das Operations Center sind die folgenden IBM Spectrum Protect-Administrator-IDs erforderlich:

Auf dem Hub-Server registrierte Administrator-IDs

Jede Administrator-ID, die auf dem Hub-Server registriert ist, kann für die Anmeldung beim Operations Center verwendet werden. Die Berechtigungsstufe der ID bestimmt die Tasks, die ausgeführt werden können. Sie können neue Administrator-IDs mit dem Befehl **REGISTER ADMIN** erstellen.

Einschränkung: Um eine Administrator-ID in einer serverübergreifenden Konfiguration verwenden zu können, muss die ID mit demselben Kennwort und derselben Berechtigungsstufe auf dem Hub-Server und den Peripherieservern registriert werden.

Die Authentifizierung für diese Server können Sie mit einer der folgenden Methoden verwalten:

- Mit einem LDAP-Server (LDAP = Lightweight Directory Access Protocol).
- Mit den Funktionen für die unternehmensweite Konfiguration, mit denen Änderungen an den Administratordefinitionen automatisch verteilt werden.

Überwachungsadministrator-ID

Wenn Sie den Hub-Server anfänglich konfigurieren, wird eine Administrator-ID mit dem Namen IBM-OC-*Servername* mit Systemberechtigung auf dem Hub-Server registriert und dem von Ihnen angegebenen Anfangskennwort zugeordnet. Diese ID, die manchmal als *Überwachungsadministrator* bezeichnet wird, ist nur für die Verwendung durch das Operations Center bestimmt.

Sie dürfen diese ID nicht löschen, sperren oder ändern. Dieselbe Administrator-ID mit demselben Kennwort wird auf den Peripherieservern registriert, die Sie hinzufügen. Das Kennwort wird automatisch alle 90 Tage auf dem Hub-Server und den Peripherieservern geändert. Sie müssen dieses Kennwort nicht verwenden oder verwalten.

Einschränkung: Das Operations Center verwaltet die ID und das Kennwort des Überwachungsadministrators auf Peripherieservern, falls Sie diese Berechtigungsnachweise nicht mithilfe einer unternehmensweiten Konfiguration verwalten. Weitere Informationen zur Verwaltung der Berechtigungsnachweise mithilfe einer unternehmensweiten Konfiguration finden Sie in „Tipps für das Entwerfen der Hub- und Peripherieserverkonfiguration" auf Seite 137.

IBM Installation Manager

Das Operations Center verwendet IBM Installation Manager, ein Installationsprogramm, mit dem viele IBM Produkte mithilfe ferner oder lokaler Software-Repositorys installiert oder aktualisiert werden können.

Wenn die erforderliche Version von IBM Installation Manager nicht bereits installiert ist, wird sie automatisch installiert oder aktualisiert, wenn Sie das Operations Center installieren. Die Software muss auf dem System installiert bleiben, damit das Operations Center später nach Bedarf aktualisiert oder deinstalliert werden kann.

Die folgende Liste enthält Erläuterungen einiger Begriffe, die in IBM Installation Manager verwendet werden:

Angebot
Eine installierbare Einheit eines Softwareprodukts.

Das Angebot 'Operations Center' enthält alle Datenträger, die IBM Installation Manager für die Installation des Operations Center benötigt.

Paket
Die Gruppe der Softwarekomponenten, die für die Installation eines Angebots benötigt werden.

Das Operations Center-Paket enthält folgende Komponenten:

- Installationsprogramm von IBM Installation Manager
- Das Angebot 'Operations Center'

Paketgruppe
Eine Gruppe von Paketen mit demselben übergeordneten Verzeichnis.

Repository
Ein ferner oder lokaler Speicherbereich für Daten und andere Anwendungsressourcen.

Das Operations Center-Paket wird in einem Repository in IBM Fix Central gespeichert.

Verzeichnis für gemeinsam genutzte Ressourcen
Ein Verzeichnis, das Softwaredateien oder Plug-ins enthält, die von Paketen gemeinsam genutzt werden.

In dem Verzeichnis für gemeinsam genutzte Ressourcen speichert IBM Installation Manager installationsbezogene Dateien, darunter Dateien, die für das Rollback zu einer vorherigen Version des Operations Center verwendet werden.

Prüfliste für die Installation

Bevor Sie das Operations Center installieren, müssen Sie bestimmte Informationen überprüfen, z. B. die Berechtigungsnachweise für die Installation, und Sie müssen die Eingabedaten festlegen, die in IBM Installation Manager für die Installation angegeben werden sollen.

Die folgende Prüfliste enthält eine Zusammenfassung der Informationen, die Sie überprüfen bzw. festlegen müssen, bevor Sie das Operations Center installieren. In Tabelle 28 auf Seite 145 werden diese Informationen dann ausführlich beschrieben.

__ Den Hostnamen des Computers überprüfen, auf dem das Operations Center installiert werden soll.
__ Die Berechtigungsnachweise für die Installation überprüfen.
__ Das Installationsverzeichnis für das Operations Center festlegen, wenn der Standardpfad nicht übernommen werden soll.
__ Das Installationsverzeichnis für IBM Installation Manager festlegen, wenn der Standardpfad nicht übernommen werden soll.
__ Die vom Operations Center zu verwendende Anschlussnummer festlegen, wenn die Standardanschlussnummer nicht übernommen werden soll.
__ Das Kennwort für die sichere Kommunikation festlegen.

Tabelle 28. Vor der Installation des Operations Center zu überprüfende bzw. festzulegende Informationen

Informationen	Details
Hostname des Computers, auf dem das Operations Center installiert werden soll.	Der Hostname muss die folgenden Kriterien erfüllen: • Der Name darf keine Zeichen aus Doppelbytezeichensätzen (DBCS) und keine Unterstreichungszeichen (_) enthalten. • Der Hostname darf zwar einen Bindestrich (-) enthalten, jedoch nicht als letztes Zeichen.
Berechtigungsnachweise für die Installation	Für die Installation des Operations Center müssen Sie das folgende Benutzerkonto verwenden: • Rootbenutzer

Operations Center-Installationsverzeichnis	Das Operations Center wird im Unterverzeichnis `ui` des Installationsverzeichnisses installiert.
	Der folgende Pfad ist der Standardpfad für das Operations Center-Installationsverzeichnis:
	• `/opt/tivoli/tsm`
	Wenn Sie beispielsweise diesen Standardpfad verwenden, wird das Operations Center in dem folgenden Verzeichnis installiert:
	`/opt/tivoli/tsm/ui`
	Der Installationsverzeichnispfad muss die folgenden Kriterien erfüllen:
	• Der Pfad darf maximal 128 Zeichen enthalten.
	• Der Pfad darf nur ASCII-Zeichen enthalten.
	• Der Pfad darf keine nicht anzeigbaren Steuerzeichen enthalten.
	• Der Pfad darf keines der folgenden Zeichen enthalten:
	`% | < > ' " $ & ; *`

IBM Installation Manager-Installationsverzeichnis	Der folgende Pfad ist der Standardpfad für das IBM Installation Manager-Installationsverzeichnis: • `/opt/IBM/InstallationManager`

Tabelle 28. Vor der Installation des Operations Center zu überprüfende bzw. festzulegende Informationen (Forts.)

Informationen	Details
Vom Operations Center-Web-Server verwendete Anschlussnummer.	Der Wert für die sichere (HTTPS) Anschlussnummer muss die folgenden Kriterien erfüllen: • Die Nummer muss eine ganze Zahl im Bereich von 1024 bis 65535 sein. • Die Nummer darf nicht bereits im Gebrauch oder anderen Programmen zugeordnet sein. Wenn Sie keine Anschlussnummer angeben, lautet der Standardwert 11090. **Tipps:** • Sie müssen zwar eine ganze Zahl im Bereich von 1024 bis 65535 angeben, aber Sie können später im Operations Center die Verwendung des sicheren TCP/IP-Standardanschlusses (443) konfigurieren. Weitere Informationen finden Sie in „Verwendung des sicheren TCP/IP-Standardanschlusses im Operations Center konfigurieren" auf Seite 158. • Wenn Sie sich später nicht mehr an die angegebene Anschlussnummer erinnern können, schauen Sie in der folgenden Datei nach (*Installationsverzeichnis* steht für das Verzeichnis, in dem das Operations Center installiert ist): – *Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer/bootstrap.properties Die Datei bootstrap.properties enthält die Verbindungsdaten des IBM Spectrum Protect-Servers.
Kennwort für die sichere Kommunikation	Das Operations Center verwendet HTTPS (Hypertext Transfer Protocol Secure) für die Kommunikation mit Web-Browsern. Für das Operations Center ist die sichere Kommunikation zwischen dem Server und dem Operations Center erforderlich. Um die Kommunikation zu schützen, müssen Sie das TLS-Zertifikat des Hub-Servers zur Truststore-Datei des Operations Center hinzufügen (TLS = Transport Layer Security). Die Truststore-Datei des Operations Center enthält das Zertifikat, das das Operations Center für die HTTPS-Kommunikation mit Web-Browsern verwendet. Während der Installation des Operations Center erstellen Sie ein Kennwort für die Truststore-Datei. Wenn Sie die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server einrichten zu können, müssen Sie dasselbe Kennwort verwenden, um das Zertifikat des Hub-Servers der Truststore-Datei hinzuzufügen. Das Kennwort für die Truststore-Datei muss die folgenden Kriterien erfüllen: • Das Kennwort darf mindestens 6 Zeichen und maximal 64 Zeichen enthalten. • Das Kennwort muss mindestens die folgenden Zeichen enthalten: – Einen Großbuchstaben (A – Z) – Einen Kleinbuchstaben (a – z) – Eine Ziffer (0 – 9) – Zwei der nachfolgend aufgelisteten nicht alphanumerischen Zeichen: `~ @ # $ % ^ & * _ - + = ` |` `( ) { } [ ] : ; < > , . ? /`

Kapitel 9. Operations Center installieren

Sie können das Operations Center mit jeder der folgenden Methoden installieren: grafischer Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

Vorbereitende Schritte

Sie können das Operations Center erst konfigurieren, nachdem Sie den IBM Spectrum Protect-Server installiert, konfiguriert und gestartet haben. Daher installieren Sie vor der Installation des Operations Center das entsprechende Serverpaket gemäß den in „Voraussetzungen für Hub- und Peripherieserver" auf Seite 136 aufgeführten Voraussetzungen bezüglich der Serverversion.

Sie können das Operations Center auf demselben Computer wie den IBM Spectrum Protect-Server oder auf einem separaten Computer installieren.

Operations Center-Installationspaket abrufen

Das Installationspaket kann von einer IBM Download-Site heruntergeladen werden, z. B. IBM Passport Advantage oder IBM Fix Central.

Informationen zu diesem Vorgang

Nachdem Sie das Paket von einer IBM Download-Site abgerufen haben, müssen Sie die Installationsdateien extrahieren.

Vorgehensweise

Gehen Sie wie folgt vor, um die Installationsdateien für das Operations Center zu extrahieren. In den folgenden Schritten müssen Sie *Versionsnummer* durch die zu installierende Version des Operations Center ersetzen.

a. Laden Sie eine der folgenden Paketdateien in ein beliebiges Verzeichnis herunter:
   - *Versionsnummer*.000-IBM-SPOC-LinuxS390.bin
   - *Versionsnummer*.000-IBM-SPOC-Linuxx86_64.bin

b. Stellen Sie sicher, dass Sie über die Ausführberechtigung für die Paketdatei verfügen.

   Bei Bedarf können Sie die Dateiberechtigungen mit dem folgenden Befehl ändern:

   ```
   chmod a+x Paketname.bin
   ```

c. Geben Sie den folgenden Befehl aus, um die Installationsdateien zu extrahieren:

   ```
   ./Paketname.bin
   ```

   Die sich selbst entpackende Paketdatei wird in das Verzeichnis extrahiert.

Operations Center mit einem grafisch orientierten Assistenten installieren

Sie können das Operations Center mithilfe des grafisch orientierten Assistenten von IBM Installation Manager installieren oder aktualisieren.

Vorgehensweise

1. Geben Sie in dem Verzeichnis, in dem die Operations Center-Installationspaketdatei extrahiert wurde, den folgenden Befehl aus:

```
./install.sh
```

2. Führen Sie die Installation der IBM Installation Manager- und Operations Center-Pakete gemäß den Anweisungen des Assistenten aus.

Nächste Schritte

Siehe „Operations Center konfigurieren” auf Seite 153.

Operations Center im Konsolenmodus installieren

Sie können das Operations Center mithilfe der Befehlszeile im Konsolenmodus installieren oder aktualisieren.

Vorgehensweise

1. Führen Sie in dem Verzeichnis, in dem die Installationspaketdatei extrahiert wurde, das folgende Programm aus:

```
./install.sh -c
```

2. Befolgen Sie die an der Konsole angezeigten Anweisungen, um die Pakete für Installation Manager und das Operations Center zu installieren.

Nächste Schritte

Siehe „Operations Center konfigurieren” auf Seite 153.

Operations Center im unbeaufsichtigten Modus installieren

Sie können das Operations Center im unbeaufsichtigten Modus installieren oder aktualisieren. Im unbeaufsichtigten Modus werden bei der Installation Nachrichten nicht an die Konsole gesendet, sondern sie werden wie auch Fehlernachrichten in Protokolldateien gespeichert.

Vorbereitende Schritte

Für die Dateneingabe bei Verwendung der unbeaufsichtigten Installation können Sie eine Antwortdatei verwenden. Die folgenden Musterantwortdateien stehen im Verzeichnis `input` zur Verfügung, in dem das Installationspaket extrahiert wird:

`install_response_sample.xml`
Verwenden Sie diese Datei für die Installation des Operations Center.

`update_response_sample.xml`
Verwenden Sie diese Datei für das Upgrade des Operations Center.

Diese Dateien enthalten Standardwerte, die dazu beitragen können, unnötige Warnungen zu vermeiden. Befolgen Sie die in den Dateien enthaltenen Anweisungen zur Verwendung dieser Dateien.

Wenn Sie eine Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

Vorgehensweise

1. Erstellen Sie eine Antwortdatei.

   Sie können die Musterantwortdatei ändern oder eine eigene Datei erstellen.

   Tipp: Zum Generieren einer Antwortdatei im Rahmen einer Installation im Konsolenmodus wählen Sie die Installationsoptionen im Konsolenmodus aus. Dann geben Sie in der Anzeige **Zusammenfassung** G ein, um die Antwortdatei entsprechend den zuvor ausgewählten Optionen zu generieren.
2. Erstellen Sie in der Antwortdatei ein Kennwort für den Truststore des Operations Center.

Wenn Sie die Datei `install_response_sample.xml` verwenden, fügen Sie das Kennwort in die folgende Zeile der Datei ein. Hierbei ist *`mein_Kennwort`* das Kennwort:

```
<variable name='ssl.password' value='mein_Kennwort'/>
```

Weitere Informationen zu diesem Kennwort finden Sie in „Prüfliste für die Installation” auf Seite 144.

Befolgen Sie die Anweisungen in „Kennwörter in Antwortdateien für unbeaufsichtigte Installation verschlüsseln” auf Seite 149, um das Kennwort zu verschlüsseln.

Tipp: Das Truststore-Kennwort ist nicht erforderlich, wenn Sie das Operations Center mit der Datei `update_response_sample.xml` aktualisieren.

3. Geben Sie den folgenden Befehl in dem Verzeichnis, in dem das Installationspaket extrahiert wurde, aus, um die unbeaufsichtigte Installation zu starten. Der Wert *Antwortdatei* gibt den Pfad und den Namen der Antwortdatei an.

   - `./install.sh -s -input Antwortdatei -acceptLicense`

Nächste Schritte

Siehe „Operations Center konfigurieren” auf Seite 153.

Kennwörter in Antwortdateien für unbeaufsichtigte Installation verschlüsseln

Um die Sicherheit während einer unbeaufsichtigten Installation des Operations Center zu erhöhen, können Sie das Kennwort in der Antwortdatei verschlüsseln. Es kann nur ein Kennwort (verschlüsselt oder unverschlüsselt) im Feld 'data key' der Antwortdatei aufgeführt werden.

Vorbereitende Schritte

Öffnen Sie IBM Installation Manager. Wechseln Sie in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das Unterverzeichnis `eclipse`. Die Standardposition des Unterverzeichnisses lautet:

`/opt/IBM/InstallationManager/eclipse`

Vorgehensweise

Führen Sie die folgenden Schritte aus, um das Kennwort in der Antwortdatei zu verschlüsseln, die für die unbeaufsichtigte Installation des Operations Center verwendet wird, und um sicherzustellen, dass nur ein Kennwort im Feld 'data key' verwendet wird:

1. Wenn Sie das Operations Center als Rootbenutzer installieren, wechseln Sie in das Unterverzeichnis tools. Die Standardposition des Unterverzeichnisses tools lautet:

   `/opt/IBM/InstallationManager/eclipse/tools`

   Wenn Sie das Operations Center als Benutzer ohne Rootberechtigung installieren, wechseln Sie in das folgende Unterverzeichnis:

   `/home/`*`Benutzer_ohne_Rootberechtigung`*`/IBM/InstallationManager/eclipse/tools`

   Hierbei gibt *Benutzer_ohne_Rootberechtigung* die Instanzbenutzer-ID an.
2. Geben Sie den folgenden Befehl in einer Zeile ein:

   ```
   ./IBMIM -silent -noSplash encryptString zu_verschlüssende_Zeichenfolge
   >verschlüsseltes_Kennwort
   ```

   Hierbei steht *zu_verschlüssende_Zeichenfolge* für den zu verschlüssenden Wert und *verschlüsseltes_Kennwort* für die Datei, die den verschlüsselten Wert enthält.

3. Öffnen Sie die verschlüsselte Kennwortdatei und kopieren Sie den Wert in das Feld 'data key' der Antwortdatei. Entfernen Sie anschließend die verschlüsselte Kennwortdatei, indem Sie sie auf Kommentar setzen.
4. Führen Sie die folgenden Schritte aus, um das nicht verschlüsselte Kennwort aus dem Feld 'data key' zu entfernen:
   a. Setzen Sie das nicht verschlüsselte Kennwort (`user.SSL_PASSWORD`) auf Kommentar, so dass die Kennwortzeile etwa wie folgt aussieht:

      ```
      <!-- <data key='user.SSL_PASSWORD' value='${ssl.password}'/> -->
      ```

   b. Entfernen Sie die Kommentarzeichen vom verschlüsselten Kennwort (`user.SSL_PASSWORD_ENCRYPTED`), so dass die Kennwortzeilen etwa wie in dem folgenden Beispiel aussehen:

      ```
      <data key='user.enableSP800_131' value='${enable.SP800131a}'/>
       <data key='user.SSL_PASSWORD_ENCRYPTED' value='${ssl.password.encrypted}'/>
      ```

   Einschränkung: Verwenden Sie nur einen Wert im Feld 'data key' der Antwortdatei, entweder `user.SSL_PASSWORD` oder `user.SSL_PASSWORD_ENCRYPTED`. Den nicht verwendeten Wert müssen Sie auf Kommentar setzen. Anderfalls erhalten Sie eine Fehlernachricht und die Installation schlägt fehl.

Beispiel

Verschlüsseln Sie das Kennwort passw0rd mit dem Installation Manager-Befehlszeilentool. Speichern Sie den verschlüsselten Wert in der Datei `my_pwd.txt`. Geben Sie den folgenden Befehl aus:

```
./IBMIM -silent -noSplash encryptString passw0rd > my_pwd.txt
```

Die Datei `my_pwd.txt` enthält den verschlüsselten Wert *rbN1IaMAWYYtQxLf6KdNyA==*:

```
<variable name='ssl.password.encrypted' value=' rbN1IaMAWYYtQxLf6KdNyA==' />
```

Kapitel 10. Upgrade des Operations Center

Sie können ein Upgrade des Operations Center mit jeder der folgenden Methoden durchführen: grafisch orientierter Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

Vorbereitende Schritte

Bevor Sie ein Upgrade des Operations Center durchführen, lesen Sie die Informationen zu den Systemvoraussetzungen und die Prüfliste für die Installation. Die Voraussetzungen und Anforderungen der neuen Version des Operations Center können von denen der momentan verwendeten Version abweichen.

Informationen zu diesem Vorgang

Die Anweisungen für das Upgrade des Operations Center sind mit Ausnahme der folgenden Punkte mit den Anweisungen für die Installation des Operations Center identisch:

- Sie verwenden nicht die Funktion **Installieren** von IBM Installation Manager, sondern die Funktion **Aktualisieren**.

  Tipp: In IBM Installation Manager bedeutet *aktualisieren* das Erkennen und Installieren von Aktualisierungen und Fixes für installierte Softwarepakete. In diesem Kontext sind *Aktualisierung* und *Upgrade* gleichbedeutend.
- Wenn Sie ein Upgrade des Operations Center im unbeaufsichtigten Modus durchführen, können Sie den Schritt für die Erstellung eines Kennworts für die Truststore-Datei überspringen.

Kapitel 11. Erste Schritte mit dem Operations Center

Bevor Sie das Operations Center für die Verwaltung Ihrer Speicherumgebung verwenden können, müssen Sie es konfigurieren.

Informationen zu diesem Vorgang

Führen Sie nach der Installation des Operations Center die folgenden Basiskonfigurationsschritte aus:

1. Legen Sie den Hub-Server fest.
2. Fügen Sie alle Peripherieserver hinzu.
3. Konfigurieren Sie wahlweise E-Mail-Alerts auf den Hub- und Peripherieservern.

Abbildung 1 auf Seite 153 veranschaulicht eine Operations Center-Konfiguration.

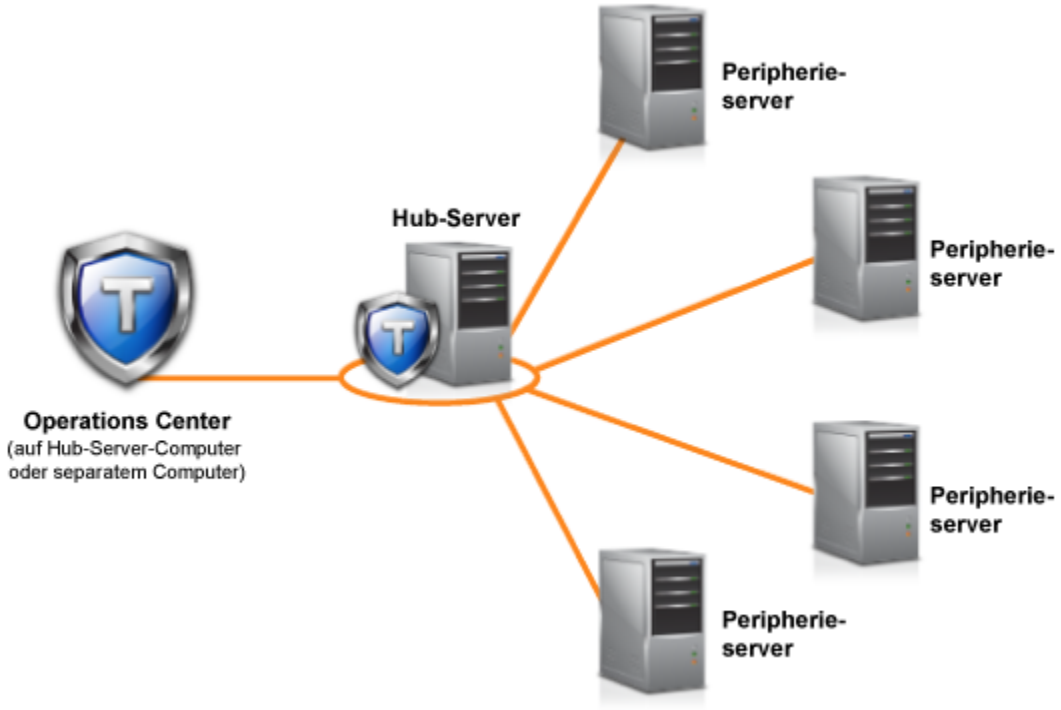


Abbildung 1. Beispiel einer Operations Center-Konfiguration mit Hub- und Peripherieservern

Operations Center konfigurieren

Wenn Sie das Operations Center zum ersten Mal öffnen, müssen Sie es für die Verwaltung Ihrer Speicherumgebung konfigurieren. Sie müssen das Operations Center dem IBM Spectrum Protect-Server zuordnen, der als Hub-Server festgelegt ist. Anschließend können Sie weitere IBM Spectrum Protect-Server als Peripherieserver verbinden.

Hub-Server festlegen

Wenn Sie zum ersten Mal eine Verbindung zum Operations Center herstellen, müssen Sie angeben, welcher IBM Spectrum Protect-Server der Hub-Server ist.

Vorbereitende Schritte

Für das Operations Center ist die sichere Kommunikation zwischen dem Hub-Server und dem Operations Center erforderlich. Um die Kommunikation zu schützen, müssen Sie das TLS-Zertifikat des Hub-Servers

zur Truststore-Datei des Operations Center hinzufügen (TLS = Transport Layer Security). Weitere Informationen finden Sie in „Kommunikation zwischen Operations Center und Hub-Server mithilfe selbst signierter Zertifikate schützen” auf Seite 160.

Vorgehensweise

Geben Sie die folgende Adresse in einem Web-Browser an. Dabei steht *Hostname* für den Namen des Computers, auf dem das Operations Center installiert ist, und *sicherer_Anschluss* für die Anschlussnummer, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet:

```
https://Hostname:sicherer_Anschluss/oc
```

Tipps:

- Bei der URL muss die Groß-/Kleinschreibung beachtet werden. Achten Sie beispielsweise darauf, dass Sie "oc" wie gezeigt in Kleinbuchstaben eingeben.
- Weitere Informationen zu der Anschlussnummer finden Sie in Prüfliste für die Installation.
- Wenn Sie zum ersten Mal eine Verbindung zum Operations Center herstellen, müssen Sie folgende Informationen angeben:
  - Verbindungsdaten für den Server, den Sie als Hub-Server festlegen wollen.
  - Berechtigungsnachweise zur Anmeldung für eine Administrator-ID, die für diesen Server definiert ist.
- Ist der Aufbewahrungszeitraum für Ereignisdatensätze des Servers kürzer als 14 Tage, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Hub-Server konfigurieren.

Nächste Schritte

Wenn Ihre Umgebung mehrere IBM Spectrum Protect-Server umfasst, fügen Sie die übrigen Server dem Hub-Server als Peripherieserver hinzu.

Achtung: Nachdem ein Server als Hub- oder Peripherieserver konfiguriert wurde, dürfen Sie seinen Namen nicht mehr ändern.

Peripherieserver hinzufügen

Nachdem Sie den Hub-Server für das Operations Center konfiguriert haben, können Sie dem Hub-Server einen oder mehrere Peripherieserver hinzufügen.

Vorbereitende Schritte

Die Kommunikation zwischen dem Peripherieserver und dem Hub-Server muss unter Verwendung des Protokolls Transport Layer Security (TLS) geschützt werden. Um die sichere Kommunikation zu ermöglichen, fügen Sie das Zertifikat des Peripherieservers der Truststore-Datei des Hub-Servers hinzu.

Vorgehensweise

1. Klicken Sie in der Menüleiste des Operations Center auf **Server**.

   Die Seite **Server** wird geöffnet.

   In der Tabelle auf der Seite **Server** könnte ein Server den Status "Nicht überwacht" haben. Dieser Status bedeutet, dass - obwohl ein Administrator diesen Server mit dem Befehl **DEFINE SERVER** für den Hub-Server definiert hat - der Server noch nicht als Peripherieserver konfiguriert ist.
2. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf den Server, um ihn hervorzuheben, und klicken Sie in der Menüleiste der Tabelle auf **Peripherieserver überwachen**.
   - Wenn der Server, der hinzugefügt werden soll, in der Tabelle nicht angezeigt wird und die sichere SSL-/TLS-Kommunikation nicht erforderlich ist, klicken Sie in der Menüleiste der Tabelle auf **+Peripherieserver**.

3. Geben Sie die erforderlichen Informationen an und führen Sie die Schritte im Konfigurationsassistenten für den Peripherieserver aus.

   Tipp: Wenn der Aufbewahrungszeitraum für Ereignissätze des Servers weniger als 14 Tage beträgt, wird der Zeitraum automatisch auf 14 Tage zurückgesetzt, wenn Sie den Server als Peripherieserver konfigurieren.

E-Mail-Alerts an Administratoren senden

Ein Alert ist eine Benachrichtigung über ein relevantes Problem auf dem IBM Spectrum Protect-Server und wird durch eine Servernachricht ausgelöst. Alerts können im Operations Center angezeigt und vom Server per E-Mail an Administratoren gesendet werden.

Vorbereitende Schritte

Bevor Sie die E-Mail-Benachrichtigung für Administratoren wegen Alerts konfigurieren, stellen Sie sicher, dass folgende Anforderungen erfüllt sind:

- Damit Alerts als E-Mail gesendet und empfangen werden können, ist ein SMTP-Server erforderlich und der Server, der die Alerts als E-Mail sendet, muss auf den SMTP-Server zugreifen können.

  Tipp: Wenn das Operations Center auf einem separaten Computer installiert ist, benötigt dieser Computer keinen Zugriff auf den SMTP-Server.
- Ein Administrator benötigt die Systemberechtigung, um die E-Mail-Benachrichtigung konfigurieren zu können.

Informationen zu diesem Vorgang

Eine E-Mail-Benachrichtigung wird nur für das erste Auftreten eines Alerts gesendet. Außerdem wird keine E-Mail-Benachrichtigung für einen Alert gesendet, wenn der Alert vor der Konfiguration der E-Mail-Benachrichtigung generiert wird.

Sie können die E-Mail-Benachrichtigung wie folgt konfigurieren:

- Benachrichtigung für einzelne Alerts senden
- Alertzusammenfassungen senden

Eine Alertzusammenfassung enthält Informationen zu aktuellen Alerts. Die Zusammenfassung beinhaltet die Gesamtzahl der Alerts, die Gesamtzahl der aktiven und inaktiven Alerts, den ältesten Alert, den neuesten Alert und den am häufigsten auftretenden Alert.

Sie können maximal drei Administratoren als Empfänger von Alertzusammenfassungen per E-Mail angeben. Alertzusammenfassungen werden ca. einmal stündlich gesendet.

Vorgehensweise

Gehen Sie auf jedem Hub- und Peripherieserver, von dem Sie E-Mail-Alerts erhalten wollen, wie folgt vor, um die E-Mail-Benachrichtigung für Administratoren wegen Alerts zu konfigurieren:

1. Geben Sie den folgenden Befehl aus, um zu überprüfen, dass die Alertüberwachung aktiviert ist:

   ```
   QUERY MONITORSETTINGS
   ```

2. Geben Sie den folgenden Befehl aus, wenn die Befehlsausgabe anzeigt, dass die Alertüberwachung inaktiviert ist. Andernfalls fahren Sie mit dem nächsten Schritt fort.

   ```
   SET ALERTMONITOR ON
   ```

3. Geben Sie den folgenden Befehl aus, um das Senden von E-Mail-Benachrichtigungen zu aktivieren:

   ```
   SET ALERTEMAIL ON
   ```

4. Geben Sie den folgenden Befehl aus, um den SMTP-Server zu definieren, der zum Senden von E-Mail-Benachrichtigungen verwendet wird:

   ```
   SET ALERTEMAILSMTPHOST Hostname
   ```

5. Geben Sie den folgenden Befehl aus, um die Anschlussnummer für den SMTP-Server anzugeben:

   ```
   SET ALERTEMAILSMTPPORT Anschlussnummer
   ```

   Die Standardanschlussnummer ist 25.

6. Geben Sie den folgenden Befehl aus, um die E-Mail-Adresse des Absenders der Alerts anzugeben:

   ```
   SET ALERTEMAILFROMADDR E-Mail-Adresse
   ```

7. Geben Sie für jede Administrator-ID, die E-Mail-Benachrichtigungen empfangen soll, einen der folgenden Befehle aus, um die E-Mail-Benachrichtigung zu aktivieren und um die E-Mail-Adresse anzugeben:

   ```
   REGISTER ADMIN Administratorname ALERT=YES EMAILADDRESS=E-Mail-Adresse
   ```

   ```
   UPDATE ADMIN Administratorname ALERT=YES EMAILADDRESS=E-Mail-Adresse
   ```

8. Wählen Sie eine oder beide der folgenden Optionen aus und geben Sie die Administrator-IDs an, die E-Mail-Benachrichtigungen empfangen sollen:

   - Benachrichtigung für einzelne Alerts senden

     Geben Sie einen der folgenden Befehle aus, um die Administrator-IDs anzugeben bzw. zu aktualisieren, die E-Mail-Benachrichtigungen für einen einzelnen Alert empfangen sollen:

     ```
     DEFINE ALERTTRIGGER Nachrichtennummer ADmin=Administratorname1,Administratorname2
     ```

     ```
     UPDATE ALERTTRIGGER Nachrichtennummer ADDadmin=Administratorname3 DELadmin=Administratorname1
     ```

     Tipp: Auf der Seite **Alerts konfigurieren** des Operations Center können Sie die Administratoren auswählen, die E-Mail-Benachrichtigungen erhalten sollen.

   - Alertzusammenfassungen senden

     Geben Sie den folgenden Befehl aus, um die Administrator-IDs anzugeben bzw. zu aktualisieren, die Alertzusammenfassungen per E-Mail erhalten sollen:

     ```
     SET ALERTSUMMARYTOADMINS Administratorname1,Administratorname2,Administratorname3
     ```

   Gehen Sie wie folgt vor, wenn Sie Alertzusammenfassungen, aber keine Benachrichtigungen über einzelne Alerts empfangen wollen:

   a. Setzen Sie die Benachrichtigung über einzelne Alerts wie in „E-Mail-Alerts vorübergehend aussetzen” auf Seite 157 beschrieben aus.

   b. Stellen Sie sicher, dass die betreffende Administrator-ID in dem folgenden Befehl aufgelistet ist:

      ```
      SET ALERTSUMMARYTOADMINS Administratorname1,Administratorname2,Administratorname3
      ```

E-Mail-Alerts an mehrere Administratoren senden

Das folgende Beispiel zeigt die Befehle, mit denen alle Alerts für Nachricht ANR1075E in einer E-Mail an die Administratoren `myadmin`, `djadmin` und `csadmin` gesendet werden:

```
SET ALERTMONITOR ON
SET ALERTEMAIL ON
SET ALERTEMAILSMTPHOST mymailserver.domain.com
SET ALERTEMAILSMTPPORT 450
SET ALERTEMAILFROMADDR srvadmin@mydomain.com
UPDATE ADMIN myadmin ALERT=YES EMAILADDRESS=myaddr@anycompany.com
```

```
UPDATE ADMIN djadmin ALERT=YES EMAILADDRESS=djaddr@anycompany.com
UPDATE ADMIN csadmin ALERT=YES EMAILADDRESS=csaddr@anycompany.com
DEFINE ALERTTRIGGER anr0175e ADMIN=myadmin,djadmin,csadmin
```

E-Mail-Alerts vorübergehend aussetzen

E-Mail-Alerts können vorübergehend ausgesetzt werden, wenn bestimmte Situationen dies erforderlich machen. Sie möchten z. B. Alertzusammenfassungen erhalten, aber die Benachrichtigung über einzelne Alerts aussetzen oder Sie möchten die E-Mail-Benachrichtigung aussetzen, wenn ein Administrator im Urlaub ist.

Vorbereitende Schritte

Konfigurieren Sie die E-Mail-Benachrichtigung für Administratoren wie in „E-Mail-Alerts an Administratoren senden” auf Seite 155 beschrieben.

Vorgehensweise

Setzen Sie die E-Mail-Benachrichtigung für einzelne Alerts oder für Alertzusammenfassungen aus.

- Benachrichtigung über einzelne Alerts aussetzen

  Verwenden Sie eine der folgenden Methoden:

  Befehl `UPDATE ADMIN`
  Geben Sie den folgenden Befehl aus, um die E-Mail-Benachrichtigung für den Administrator zu inaktivieren:

  ```
  UPDATE ADMIN Administratorname ALERT=NO
  ```

  Geben Sie den folgenden Befehl aus, um die E-Mail-Benachrichtigung später wieder zu aktivieren:

  ```
  UPDATE ADMIN Administratorname ALERT=YES
  ```

  Befehl `UPDATE ALERTTRIGGER`
  Geben Sie den folgenden Befehl aus, um zu verhindern, dass ein bestimmter Alert an einen Administrator gesendet wird:

  ```
  UPDATE ALERTTRIGGER Nachrichtennummer DELADMIN=Administratorname
  ```

  Geben Sie den folgenden Befehl aus, damit dieser Alert wieder an den Administrator gesendet wird:

  ```
  UPDATE ALERTTRIGGER Nachrichtennummer ADDADMIN=Administratorname
  ```

- Benachrichtigung über Alertzusammenfassungen aussetzen

  Entfernen Sie die Administrator-ID aus der Liste in dem folgenden Befehl, um zu verhindern, dass Alertzusammenfassungen an einen Administrator gesendet werden:

  ```
  SET ALERTSUMMARYTOADMINS Administratorname1,Administratorname2,Administratorname3
  ```

  Wenn eine Administrator-ID in dem vorhergehenden Befehl aufgelistet ist, erhält der Administrator Alertzusammenfassungen per E-Mail, auch wenn die Benachrichtigung über einzelne Alerts für die betreffende Administrator-ID ausgesetzt ist.

Angepassten Text in die Anmeldeanzeige einfügen

Sie können angepassten Text, z. B. die Nutzungsbedingungen Ihres Unternehmens für die Software, zur Anmeldeanzeige des Operations Center hinzufügen, so dass die Benutzer des Operations Center den Text sehen, bevor sie ihren Benutzernamen und ihr Kennwort eingeben.

Vorgehensweise

Gehen Sie wie folgt vor, um angepassten Text zur Anmeldeanzeige hinzuzufügen:

1. Wechseln Sie auf dem Computer, auf dem das Operations Center installiert ist, in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):

   Installationsverzeichnis/ui/Liberty/usr/servers/guiServer
2. Erstellen Sie in dem Verzeichnis eine Datei mit dem Namen `loginText.html`, die den Text enthält, den Sie zur Anmeldeanzeige hinzufügen wollen.

   Text mit Sonderzeichen, die keine ASCII-Zeichen sind, muss UTF-8-codiert sein.
3. Überprüfen Sie den hinzugefügten Text in der Anmeldeanzeige des Operations Center.

   Geben Sie die folgende Adresse in einem Web-Browser an, um das Operations Center zu öffnen. Dabei steht *Hostname* für den Namen des Computers, auf dem das Operations Center installiert ist, und *sicherer_Anschluss* für die Anschlussnummer, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet:

   ```
   https://Hostname:sicherer_Anschluss/oc
   ```

Verwendung des sicheren TCP/IP-Standardanschlusses im Operations Center konfigurieren

Anschluss 443 ist der Standardanschluss für die sichere Web-Browser-Kommunikation. Wenn über eine Firewall auf das Operations Center zugegriffen werden muss, können Sie in der Konfiguration des Operations Center angeben, dass die Kommunikation über diesen Standardanschluss stattfinden soll. Auf diese Weise können Sie vermeiden, dass ein weiterer Anschluss in der Firewall geöffnet wird.

Informationen zu diesem Vorgang

Bei der Installation des Operations Center ist die Standardanschlussnummer für die sichere Kommunikation zwischen dem Web-Server des Operations Center und den Web-Browsern 11090. Sie können diesen Standardanschluss während der Installation akzeptieren oder eine andere Anschlussnummer im Bereich von 1024 bis 65535 angeben. Während der Installtion ist es nicht möglich, eine Anschlussnummer unter 1024 anzugeben, weil diese Anschlüsse für bestimmte Netzservices reserviert sind.

Nach der Installation des Operations Center ist der Web-Server an dem angegebenen Anschluss für Anforderungen von Web-Browsern empfangsbereit. Fall das Operations Center nicht geöffnet werden kann, weil der Anschluss von einer Firewall blockiert wird, muss der Anschluss von einem Administrator geöffnet werden, damit Browser eine Verbindung herstellen können. In einigen Produktionsumgebungen könnte es effizienter sein, den Systemanschluss 443 zu verwenden. Da dieser Systemanschluss für sicheres Web-Browsing reserviert ist, ist er wahrscheinlich bereits in der Firewall geöffnet. Sie können den Anschluss 443 zwar nicht während der Installation angeben, aber nach der Installation.

Vorgehensweise

Führen Sie die folgenden Schritte nach der Installation des Operations Center aus, um die Verwendung von Anschluss 443 für den Web-Server des Operations Center zu konfigurieren:

1. Stoppen Sie den Web-Server des Operations Center.

   Anweisungen zum Stoppen des Web-Servers finden Sie in „Web-Server starten und stoppen” auf Seite 179.
2. Wechseln Sie in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):

   Installationsverzeichnis/ui/Liberty/usr/servers/guiServer
3. Öffnen Sie die Datei `bootstrap.properties`, die eine Eigenschaft enthält, die den Anschluss angibt, den der Web-Server des Operations Center für die sichere Kommunikation verwendet.
4. Geben Sie für die Eigenschaft `tsm.https.port` den Anschluss 443 an:

```
tsm.https.port=443
```

5. Speichern und schließen Sie die Datei `bootstrap.properties`.
6. Starten Sie den Web-Server des Operations Center.

   Sie müssen das Operations Center als Rootbenutzer starten. Falls Sie das Operations Center nicht als Rootbenutzer starten, kann das Operations Center nicht über Anschluss 443 kommunizieren.

   Anweisungen zum Starten des Web-Servers des Operations Center finden Sie in „Web-Server starten und stoppen" auf Seite 179.

Nächste Schritte

Informieren Sie die Benutzer darüber, dass das Operations Center den sicheren TCP/IP-Standardanschluss verwendet. Normalerweise öffnet ein Benutzer das Operations Center im Browser mit einer URL, die die Anschlussnummer enthält. Da 443 der Standardanschluss für die sichere Web-Browser-Kommunikation ist, muss die Anschlussnummer in der URL nicht angegeben werden. Stattdessen kann die folgende URL verwendet werden, in der *Hostname* den Namen des Computers angibt, auf dem das Operations Center installiert ist:

```
https:Hostname/oc/
```

Anweisungen zum Öffnen des Operations Center finden Sie in „Operations Center öffnen" auf Seite 180.

REST-Services aktivieren

Anwendungen, die REST-Services verwenden, können die Speicherumgebung abfragen und verwalten, indem eine Verbindung zum Operations Center hergestellt wird (REST = Representational State Transfer).

Informationen zu diesem Vorgang

Aktivieren Sie dieses Feature, um REST-Services eine Interaktion mit Hub- und Peripherieservern zu ermöglichen. Dabei werden Aufrufe an die folgende Adresse gesendet:

```
https://OC-Hostname:Anschluss/oc/api
```

Hierbei steht *OC-Hostname* für den Netznamen oder die IP-Adresse des Hostsystems des Operations Center und *Anschluss* für die Anschlussnummer des Operations Center. Die Standardanschlussnummer ist 11090.

Informationen zu den für das Operations Center verfügbaren REST-Services finden Sie in Technote http://www-01.ibm.com/support/docview.wss?uid=swg21997347 oder geben Sie den folgenden REST-Aufruf aus:

```
https://OC-Hostname:Anschluss/oc/api/help
```

Vorgehensweise

1. Bewegen Sie den Mauszeiger in der Menüleiste des Operations Center über das Symbol für die Einstellungen  und klicken Sie auf **Einstellungen**.
2. Wählen Sie auf der Seite 'Allgemein' das Kontrollkästchen **Verwaltungs-REST-API aktivieren** aus.
3. Klicken Sie auf **Speichern**.

Sichere Kommunikation konfigurieren

Das Operations Center verwendet HTTPS (Hypertext Transfer Protocol Secure) für die Kommunikation mit Web-Browsern. Das TLS-Protokoll schützt die Kommunikation zwischen dem Operations Center und dem Hub-Server sowie zwischen dem Hub-Server und den zugeordneten Peripherieservern (TLS = Transport Layer Security).

Informationen zu diesem Vorgang

TLS Version 1.2 oder höher ist für die sichere Kommunikation zwischen dem IBM Spectrum Protect-Server und dem Operations Center sowie zwischen dem Hub-Server und den Peripherieservern erforderlich.

Kommunikation zwischen Operations Center und Hub-Server mithilfe selbst signierter Zertifikate schützen

Um die Kommunikation zwischen dem Operations Center und dem Hub-Server zu schützen, müssen Sie das TLS-Zertifikat (Transport Layer Security) des Hub-Servers der Truststore-Datei des Operations Center hinzufügen.

Vorbereitende Schritte

Die Truststore-Datei des Operations Center ist ein Container für Zertifikate, auf die vom Operations Center zugegriffen werden kann. Während der Installation des Operations Center müssen Sie ein Kennwort für die Truststore-Datei erstellen. Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server zu ermöglichen, müssen Sie dasselbe Kennwort verwenden, um das Zertifikat des Hub-Servers der Truststore-Datei hinzuzufügen. Wenn Sie dieses Kennwort vergessen haben, müssen Sie es jetzt erneut erstellen und die Truststore-Datei konfigurieren. Anweisungen finden Sie in Kennwort für die Truststore-Datei des Operations Center löschen und erneut zuordnen.

Die folgende Abbildung zeigt die Komponenten für die Konfiguration einer Secure Sockets Layer-(SSL-)Verbindung zwischen dem Hub-Server und dem Operations Center.

Informationen zu diesem Vorgang

Diese Prozedur stellt Schritte zur Implementierung der sicheren Kommunikation mithilfe selbst signierter Zertifikate bereit. Wenn Sie Zertifikate verwenden, die von einer Zertifizierungsstelle (certificate authority, CA) signiert wurden, lesen Sie den Abschnitt Kommunikation zwischen Operations Center und Hub-Server mithilfe CA-signierter Zertifikate schützen.

Vorgehensweise

1. Stoppen Sie den Web-Server des Operations Center.
2. Rufen Sie die Befehlszeile des Betriebssystems auf, auf dem das Operations Center installiert ist.
3. Verwenden Sie das Dienstprogramm **iKeycmd** oder **iKeyman**, um das Zertifikat der Truststore-Datei des Operations Center hinzuzufügen.

   Das Dienstprogramm **iKeycmd** ist eine Befehlszeilenschnittstelle und das Dienstprogramm **iKeyman** ist die grafische Benutzerschnittstelle von IBM Key Management.

   Die Dienstprogramme **iKeycmd** und **iKeyman** müssen als Rootbenutzer ausgeführt werden.

   Gehen Sie wie folgt vor, um das TLS-Zertifikat mithilfe der Befehlszeilenschnittstelle hinzuzufügen:

   a) Wechseln Sie in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):

   - *Installationsverzeichnis*/ui/jre/bin

b) Geben Sie den Befehl **iKeycmd** aus, um das Zertifikat `cert256.arm` des Servers dem Truststore des Operations Center hinzuzufügen.

```
ikeycmd -cert -add
-db /Installationsverzeichnis/ui/Liberty/usr/servers/guiServer/gui-truststore.jks
-file /Serverinstanzverzeichnis/cert256.arm
-label 'Kennsatzbeschreibung'
-pw 'Kennwort' -type jks -format ascii -trust enable
```

Hierbei gilt Folgendes:

Installationsverzeichnis
Das Verzeichnis, in dem das Operations Center installiert ist.

Serverinstanzverzeichnis
Das IBM Spectrum Protect-Serverinstanzverzeichnis.

Kennsatzbeschreibung
Die Beschreibung, die Sie dem Kennsatz zuordnen.

Kennwort
Das Kennwort, das Sie bei der Installation des Operations Center erstellt haben. Wenn Sie das Kennwort zurücksetzen wollen, deinstallieren Sie das Operations Center, löschen Sie die Datei `.jks` und installieren Sie das Operations Center erneut.

Gehen Sie wie folgt vor, um das Zertifikat mithilfe des Fensters '**IBM Key Management**' hinzuzufügen:

a) Wechseln Sie in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):

- *Installationsverzeichnis*/ui/jre/bin

b) Geben Sie den folgenden Befehl aus, um das Fenster **IBM Key Management** zu öffnen:

```
ikeyman
```

c) Klicken Sie auf **Schlüsseldatenbankdatei** > **Öffnen**.

d) Klicken Sie im Fenster **Öffnen** auf **Durchsuchen** und wechseln Sie in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):

- *Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer

e) Wählen Sie im Verzeichnis `guiServer` die Datei `gui-truststore.jks` aus.

f) Klicken Sie auf **Öffnen** und dann auf **OK**.

g) Geben Sie das Kennwort für die Truststore-Datei ein und klicken Sie auf **OK**.

h) Klicken Sie im Bereich **Schlüsseldatenbankinhalt** des Fensters **IBM Key Management** auf den Pfeil und wählen Sie **Zertifikate des Unterzeichners** in der Liste aus.

i) Klicken Sie auf **Hinzufügen**.

j) Klicken Sie im Fenster **Öffnen** auf **Durchsuchen** und wechseln Sie in das Verzeichnis der Hub-Server-Instanz. Dieses Verzeichnis enthält das Zertifikat `cert256.arm`.

Wenn Sie im Fenster **Öffnen** nicht auf das Verzeichnis der Hub-Server-Instanz zugreifen können, gehen Sie wie folgt vor:

i) Kopieren Sie die Datei `cert256.arm` mithilfe von FTP oder einer anderen Dateiübertragungsmethode aus dem Instanzverzeichnis des Hub-Servers in das folgende Verzeichnis auf dem Computer, auf dem das Operations Center installiert ist:

- *Installationsverzeichnis*/ui/Liberty/usr/servers/guiServer

ii) Wechseln Sie im Fenster **Öffnen** in das Verzeichnis `guiServer`.

k) Wählen Sie das Zertifikat `cert256.arm` aus.

Tipp: Das von Ihnen ausgewählte Zertifikat muss als Standardzertifikat in der Schlüsseldatenbankdatei des Hub-Servers definiert sein.

l) Klicken Sie auf **Öffnen** und dann auf **OK**.

m) Geben Sie eine Bezeichnung für das Zertifikat ein.
Geben Sie beispielsweise den Namen des Hub-Servers ein.

n) Klicken Sie auf **OK**.

Das SSL-Zertifikat des Hub-Servers wird der Truststore-Datei hinzugefügt und die Bezeichnung im Bereich **Schlüsseldatenbankinhalt** des Fensters **IBM Key Management** angezeigt.

o) Schließen Sie das Fenster **IBM Key Management**.

4. Starten Sie den Web-Server des Operations Center.
5. Wenn Sie zum ersten Mal eine Verbindung zum Operations Center herstellen, müssen Sie die IP-Adresse oder den Netznamen des Hub-Servers und die Anschlussnummer für die Kommunikation mit dem Hub-Server angeben. Geben Sie die durch die Serveroption TCPADMINPORT oder SSLTCPADMINPORT angegebene Anschlussnummer ein.

   Wenn das Operations Center bereits konfiguriert wurde, können Sie den Inhalt der Datei `serverConnection.properties` überprüfen, um die Verbindungsdaten zu verifizieren. Die Datei `serverConnection.properties` befindet sich in dem folgenden Verzeichnis auf dem Computer, auf dem das Operations Center installiert ist:

   • *Installationsverzeichnis*`/ui/Liberty/usr/servers/guiServer`

Nächste Schritte

Informationen zur Konfiguration der TLS-Kommunikation zwischen dem Hub-Server und einem Peripherieserver finden Sie in „Kommunikation zwischen Hub-Server und Peripherieserver schützen" auf Seite 163.

Zugehörige Tasks

„Kennwort für die Truststore-Datei des Operations Center löschen und neu zuordnen" auf Seite 178
Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server einrichten zu können, müssen Sie das Kennwort für die Truststore-Datei des Operations Center kennen. Sie erstellen dieses Kennwort während der Installation des Operations Center. Wenn Sie das Kennwort nicht kennen, können Sie es löschen und ein neues Kennwort zuordnen.

Kommunikation zwischen Operations Center und Hub-Server mithilfe CA-signierter Zertifikate schützen

Wenn Sie den Hub-Server mit CA-signierten Zertifikaten schützen, müssen die CA-Stamm- und -Zwischenzertifikatsdateien, die von der Zertifizierungsstelle (certificate authority, CA) für die Verwendung auf dem Hub-Server gesendet werden, der Truststore-Datei des Operations Center hinzugefügt werden.

Vorbereitende Schritte

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Die Truststore-Datei des Operations Center ist ein Container für Zertifikate, auf den das Operations Center zugreifen kann. Während der Installation des Operations Center müssen Sie ein Kennwort für die Truststore-Datei erstellen. Um die Kommunikation zwischen dem Operations Center und dem Hub-Server zu schützen, müssen Sie dasselbe Kennwort verwenden, um das Zertifikat des Hub-Servers der Truststore-Datei hinzuzufügen. Wenn Sie dieses Kennwort vergessen haben, müssen Sie jetzt die Truststore-Datei erneut erstellen und konfigurieren. Anweisungen siehe „Kennwort für die Truststore-Datei des Operations Center löschen und neu zuordnen" auf Seite 178.
- Sie haben die CA-signierten Zertifikate, die für eine Verbindung zum Server benötigt werden, von der Zertifizierungsstelle erhalten und auf dem Server installiert. Siehe Server zum Akzeptieren von SSL-Verbindungen konfigurieren.

Die folgende Abbildung zeigt die Komponenten für die Konfiguration einer SSL-Verbindung zwischen dem Hub-Server und dem Operations Center (SSL = Secure Sockets Layer).

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, die CA-Stamm- und -Zwischenzertifikate für jeden IBM Spectrum Protect-Server vom Hub-Server in das Operations Center zu importieren.

Tipp: Wenn Sie selbst signierte Zertifikate verwenden, die standardmäßig installiert werden, lesen Sie den Abschnitt „Kommunikation zwischen Operations Center und Hub-Server mithilfe selbst signierter Zertifikate schützen" auf Seite 160.

Vorgehensweise

1. Navigieren Sie zur Befehlszeile des Betriebssystems, auf dem das Operations Center installiert ist.
2. Wechseln Sie in der Befehlszeile zur Schlüsselspeicherposition:

   Installationsverzeichnis`/ui/Liberty/usr/servers/guiServer`

   Dabei ist *Installationsverzeichnis* das Verzeichnis, in dem das Operations Center installiert ist.
3. Kopieren Sie die Dateien des CA-Stammzertifikats und des CA-Zwischenzertifikats an diese Position.

   Tipp: Die Zertifikatsdateien wurden zuvor an die Position des Hub-Servers kopiert.
4. Stoppen Sie den Web-Server des Operations Center wie in „Web-Server starten und stoppen" auf Seite 179 beschrieben.
5. Erstellen Sie eine Sicherungskopie der Operations Center-Truststore-Datei für den Fall, dass die ursprüngliche Version wieder benötigt wird. Die Operations Center-Truststore-Datei hat den Namen `gui-truststore.jks`.
6. Verwenden Sie einen der folgenden Befehle, um die Schritte für den Empfang des CA-signierten Zertifikats auszuführen:
   - Befehl **`ikeyman`**: Rufen Sie den Abschnitt „Signiertes Zertifikat mit IBM Key Management empfangen" auf Seite 170 auf und lesen Sie die Schritte für den Empfang des signierten Zertifikats.
   - Befehl **`ikeycmd`**: Rufen Sie den Abschnitt „Signiertes Zertifikat mit ikeycmd empfangen" auf Seite 177 auf und lesen Sie die Schritte für den Empfang des signierten Zertifikats.
7. Starten Sie den Web-Server des Operations Center.

Nächste Schritte

Befolgen Sie die Anweisungen in „Kommunikation zwischen Hub-Server und Peripherieserver schützen" auf Seite 163, um die TLS-Kommunikation zwischen dem Hub-Server und einem Peripherieserver zu konfigurieren.

Zugehörige Tasks

„Signiertes Zertifikat empfangen" auf Seite 170
Die Zertifizierungsstelle muss Ihnen die Zertifikatsdatei senden, die der Truststore-Datei hinzuzufügen ist.

Kommunikation zwischen Hub-Server und Peripherieserver schützen

Sie müssen das Zertifikat des Peripherieservers im Hub-Server und das Zertifikat des Hub-Servers im Peripherieserver definieren, um die Kommunikation zwischen dem Hub-Server und einem Peripherieserver

mithilfe des TLS-Protokolls zu schützen (TLS = Transport Layer Security). Außerdem müssen Sie im Operations Center die Überwachung des Peripherieservers konfigurieren.

Informationen zu diesem Vorgang

Der Hub-Server empfängt Status- und Alertinformationen vom Peripherieserver und zeigt diese Informationen im Operations Center an. Um die Status- und Alertinformationen vom Peripherieserver empfangen zu können, muss das Zertifikat des Peripherieservers der Truststore-Datei des Hub-Servers hinzugefügt werden. Außerdem müssen Sie das Operations Center für die Überwachung des Peripherieservers konfigurieren.

Um andere Funktionen des Operations Center, wie beispielsweise die automatische Implementierung von Clientaktualisierungen, aktivieren zu können, muss das Zertifikat des Hub-Servers der Truststore-Datei des Peripherieservers hinzugefügt werden.

Vorgehensweise

1. Führen Sie die folgenden Schritte aus, um das Zertifikat des Peripherieservers für den Hub-Server zu definieren:
   a) Wechseln Sie auf dem Peripherieserver in das Verzeichnis der Peripherieserverinstanz.
   b) Überprüfen Sie die Zertifikate in der Schlüsseldatenbankdatei des Peripherieservers. Geben Sie den folgenden Befehl aus:

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

   c) Übertragen Sie die Datei `cert256.arm` des Peripherieservers sicher auf den Hub-Server.
   d) Wechseln Sie auf dem Hub-Server in das Verzeichnis der Hub-Server-Instanz.
   e) Definieren Sie das Zertifikat des Peripherieservers für den Hub-Server. Geben Sie im Verzeichnis der Hub-Server-Instanz den folgenden Befehl aus; dabei ist *Name_des_Peripherieservers* der Name des Peripherieservers und *cert256.arm_für_Peripherieserver* der Dateiname des Zertifikats des Peripherieservers:

      ```
      gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii -trust enable
       -label Name_des_Peripherieservers -file cert256.arm_für_Peripherieserver
      ```

2. Führen Sie die folgenden Schritte aus, um das Zertifikat des Hub-Servers für den Peripherieserver zu definieren:
   a) Wechseln Sie auf dem Hub-Server in das Verzeichnis der Hub-Server-Instanz.
   b) Überprüfen Sie die Zertifikate in der Schlüsseldatenbankdatei des Peripherieservers. Geben Sie den folgenden Befehl aus:

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

   c) Übertragen Sie die Datei `cert256.arm` des Hub-Servers sicher auf den Peripherieserver.
   d) Wechseln Sie auf dem Peripherieserver in das Verzeichnis der Peripherieserverinstanz.
   e) Definieren Sie das Zertifikat des Hub-Servers für den Peripherieserver. Geben Sie im Verzeichnis der Peripherieserverinstanz den folgenden Befehl aus; dabei ist *Name_des_Hub-Servers* der Name des Hub-Servers und *cert256.arm_für_Hub-Server* der Dateiname des Zertifikats des Hub-Servers:

      ```
      gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii -trust enable
       -label Name_des_Hub-Servers -file cert256.arm_für_Hub-Server
      ```

3. Starten Sie den Hub-Server und den Peripherieserver erneut.
4. Führen Sie die folgenden Schritte aus, um den Peripherieserver für den Hub-Server und den Hub-Server für den Peripherieserver zu definieren.
   a) Geben Sie die folgenden Befehle sowohl auf dem Hub-Server als auch auf dem Peripherieserver aus:

```
SET SERVERPASSWORD Serverkennwort
SET SERVERHLADDRESS IP-Adresse
SET SERVERLLADDRESS TCP-Port
```

b) Geben Sie auf dem Hub-Server den Befehl **DEFINE SERVER** gemäß dem folgenden Beispiel aus:

```
DEFINE SERVER Name_des_Peripherieservers HLA=Adresse_des_Peripherieservers
 LLA=spoke_SSLTCPADMINPort SERVERPA=Kennwort_für_Peripherieserver
```

c) Geben Sie auf dem Peripherieserver den Befehl **DEFINE SERVER** gemäß dem folgenden Beispiel aus:

```
DEFINE SERVER Name_des_Hub-Servers HLA=Adresse_des_Hub-Servers
 LLA=hub_SSLTCPADMINPort SERVERPA=Kennwort_des_Hub-Servers
```

Tipp: Standardmäßig wird die Serverkommunikation verschlüsselt, es sei denn, der Server sendet oder empfängt Objektdaten. Objektdaten werden unter Verwendung von TCP/IP gesendet und empfangen. Wenn die Objektdaten nicht verschlüsselt werden, ist die Serverleistung ähnlich wie bei der Kommunikation über eine TCP/IP-Sitzung und die Sitzung ist sicher. Um die gesamte Kommunikation mit dem angegebenen Server selbst dann zu verschlüsseln, wenn der Server Objektdaten sendet und empfängt, geben Sie den Parameter SSL=YES im Befehl **DEFINE SERVER** an.

5. Führen Sie die folgenden Schritte aus, um das Operations Center für die Überwachung des Peripherieservers zu konfigurieren:
   a) Klicken Sie in der Menüleiste des Operations Center auf **Server**.

      Der Peripherieserver hat den Status 'Nicht überwacht'. Dieser Status bedeutet, dass - obwohl dieser Server für den Hub-Server mit dem Befehl **DEFINE SERVER** definiert wurde - der Server noch nicht als Peripherieserver konfiguriert ist.

   b) Klicken Sie auf den Peripherieserver, um den Eintrag hervorzuheben, und klicken Sie auf **Peripherieserver überwachen**.

SSL-Kommunikation zwischen dem Operations Center und Web-Browsern konfigurieren

Während der Installation des Operations Center wird ein selbst signiertes digitales Zertifikat generiert und dann für Web-Browser-Sitzungen verwendet. Sie können wahlweise anstelle des selbst signierten Zertifikats ein von einer unabhängigen Zertifizierungsstelle signiertes Zertifikat verwenden.

Informationen zu diesem Vorgang

Das Operations Center verwendet immer das Protokoll HTTPS für die Kommunikation mit Web-Browsern. Die gesamte Kommunikation zwischen Ihrem Browser und dem Operations Center wird mithilfe von Version 1.2 oder höher des TLS-Protokolls verschlüsselt.

Standardmäßig wird das selbst signierte Zertifikat verwendet, um die sichere Verbindung zwischen dem Browser und dem Operations Center zu erstellen. Da das Zertifikat ein selbst signiertes Zertifikat ist, kann der Web-Browser die Identität des Servers nicht überprüfen und zeigt eine Warnung an. Selbst signierte Zertifikate werden häufig für Intranet-Websites verwendet, bei denen die Gefahr einer abgefangenen Verbindung oder eines imitierten Servers möglicherweise nicht als ernste Bedrohung angesehen wird. Sie können die Sicherheitswarnung des Browsers übergehen und das selbst signierte Zertifikat verwenden oder Sie können das selbst signierte Zertifikat durch ein Zertifikat von einer anerkannten Zertifizierungsstelle (CA) ersetzen.

Soll das selbst signierte Zertifikat verwendet werden, ist keine weitere Konfiguration erforderlich.

Soll ein von einer Zertifizierungsstelle signiertes Zertifikat verwendet werden, müssen mehrere Schritte ausgeführt werden.

Vorgehensweise

1. Erstellen Sie eine Zertifikatssignieranforderung.

2. Senden Sie die Zertifikatssignieranforderung zum Signieren an die Zertifizierungsstelle.
3. Fügen Sie das Zertifikat der Truststore-Datei des Operations Center hinzu.

Zertifikatssignieranforderung erstellen

Um ein von einem Drittanbieter signiertes Zertifikat anzufordern, müssen Sie eine Zertifikatssignieranforderung (Certificate Signing Request = CSR) erstellen, die an die Zertifizierungsstelle (CA) gesendet werden muss.

Vorbereitende Schritte

Die Truststore-Datei des Operations Center ist ein Container für SSL/TLS-Zertifikate, auf den das Operations Center zugreifen kann. Die Truststore-Datei enthält das Zertifikat, das das Operations Center für die HTTPS-Kommunikation mit Web-Browsern verwendet.

Während der Installation des Operations Center erstellen Sie ein Kennwort für die Truststore-Datei. Für die Arbeit mit der Truststore-Datei müssen Sie das Truststore-Kennwort kennen. Wenn Sie dieses Kennwort vergessen haben, befolgen Sie die Anweisungen in „Kennwort für die Truststore-Datei des Operations Center löschen und neu zuordnen” auf Seite 178.

Vorgehensweise

Gehen Sie wie folgt vor, um eine Zertifikatssignieranforderung zu erstellen:

1. Wechseln Sie in der Befehlszeile zur Schlüsselspeicherposition:

   Installationsverzeichnis/ui/Liberty/usr/servers/guiServer
2. Erstellen Sie mithilfe des Befehls **ikeyman** oder **ikeycmd** eine Zertifikatsanforderung. Der Befehl **ikeyman** öffnet die grafische Benutzerschnittstelle von IBM Key Management, und **ikeycmd** ist eine Befehlszeilenschnittstelle.

   Tipp: Sie müssen möglicherweise den vollständigen Pfad zum Befehl **ikeyman** bzw. **ikeycmd** angeben. Die Befehle befinden sich in dem folgenden Verzeichnis; dabei ist *Installationsverzeichnis* das Verzeichnis, in dem das Operations Center installiert ist:

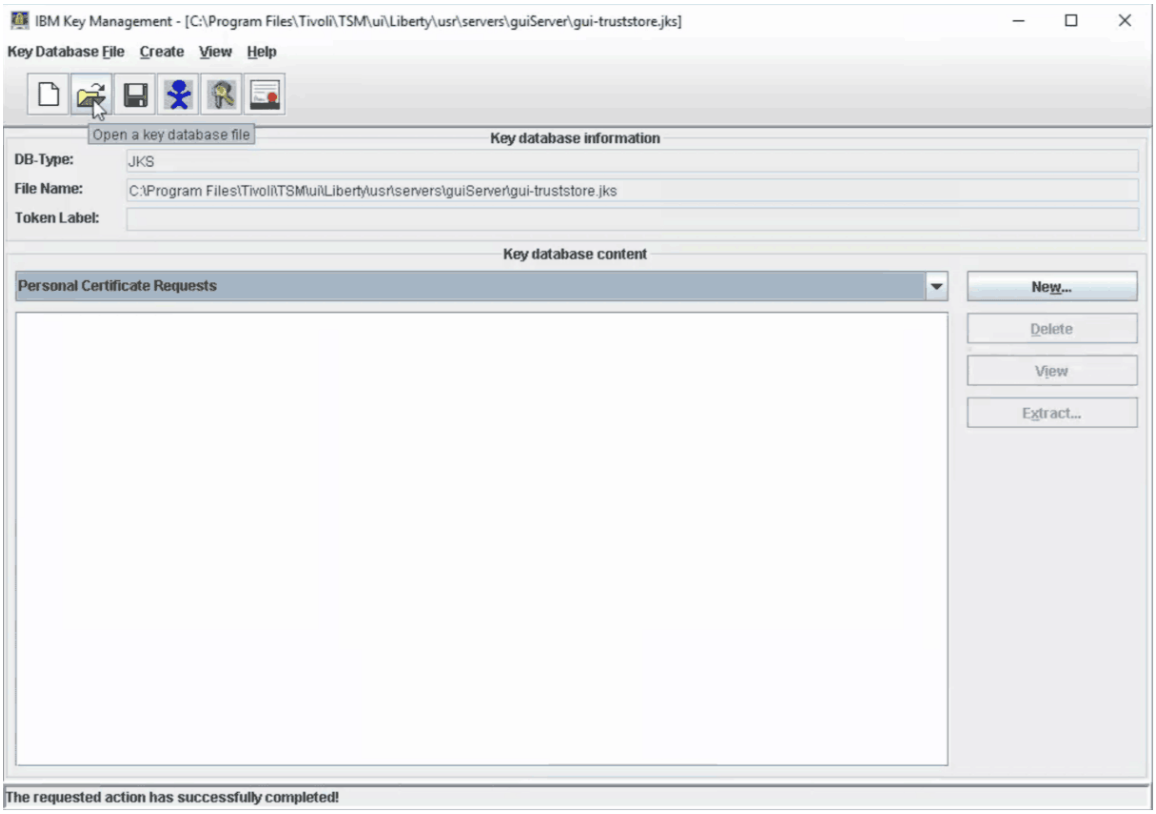
   Installationsverzeichnis/ui/jre/bin

   - Führen Sie die folgenden Schritte aus, um eine Zertifikatsanforderung mithilfe der grafischen Benutzerschnittstelle **ikeyman** zu erstellen:

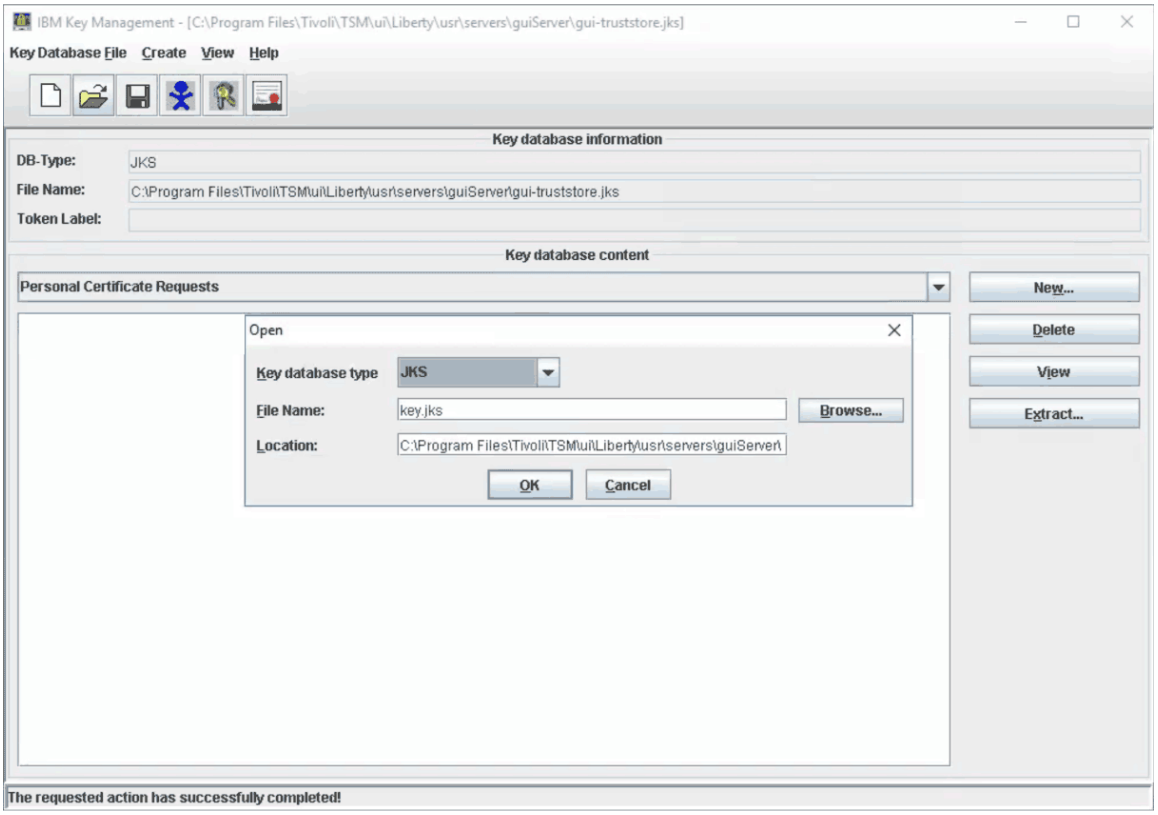
     a. Öffnen Sie das IBM Key Management-Tool, indem Sie den folgenden Befehl ausgeben:

     ```
     ikeyman
     ```

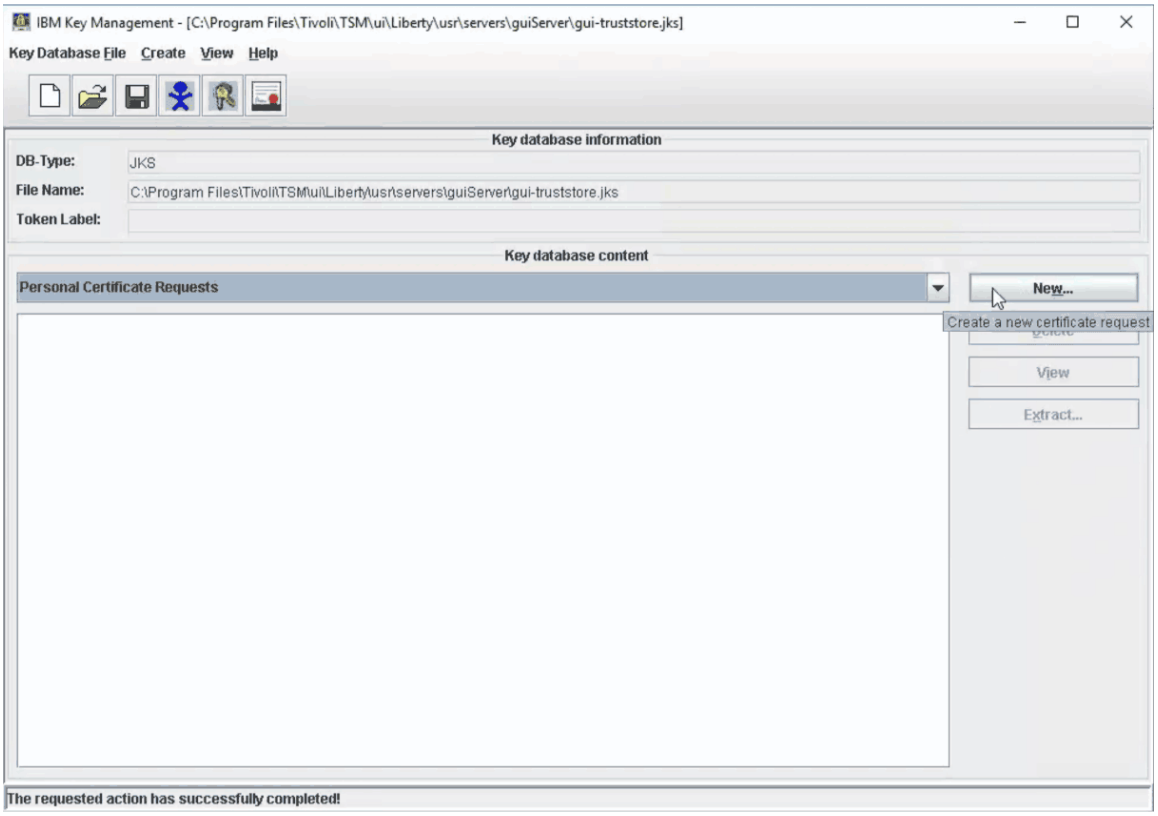
     b. Klicken Sie auf **Schlüsseldatenbankdatei** > **Öffnen**.



Klicken Sie im Fenster **Öffnen** auf **Durchsuchen**, um das Verzeichnis zu öffnen, und wählen Sie die Datei `gui-truststore.jks` aus. Klicken Sie auf **OK**.



c. Erstellen Sie eine Zertifikatsanforderung. Klicken Sie im Bereich **Schlüsseldatenbankinhalt** auf **Neu**.



d. Füllen Sie im Dialogfenster 'Neuen Schlüssel und neue Zertifikatanforderung erstellen' die Felder gemäß den Anforderungen der Zertifizierungsstelle und Ihres Unternehmens aus. Geben Sie die folgenden Informationen an:

Schlüsselkennsatz
Geben Sie einen eindeutigen Kennsatz für das Zertifikat in der Truststore-Datei an. Der Kennsatzname (z. B. *usr-cert-name*) identifiziert das Zertifikat im Truststore.

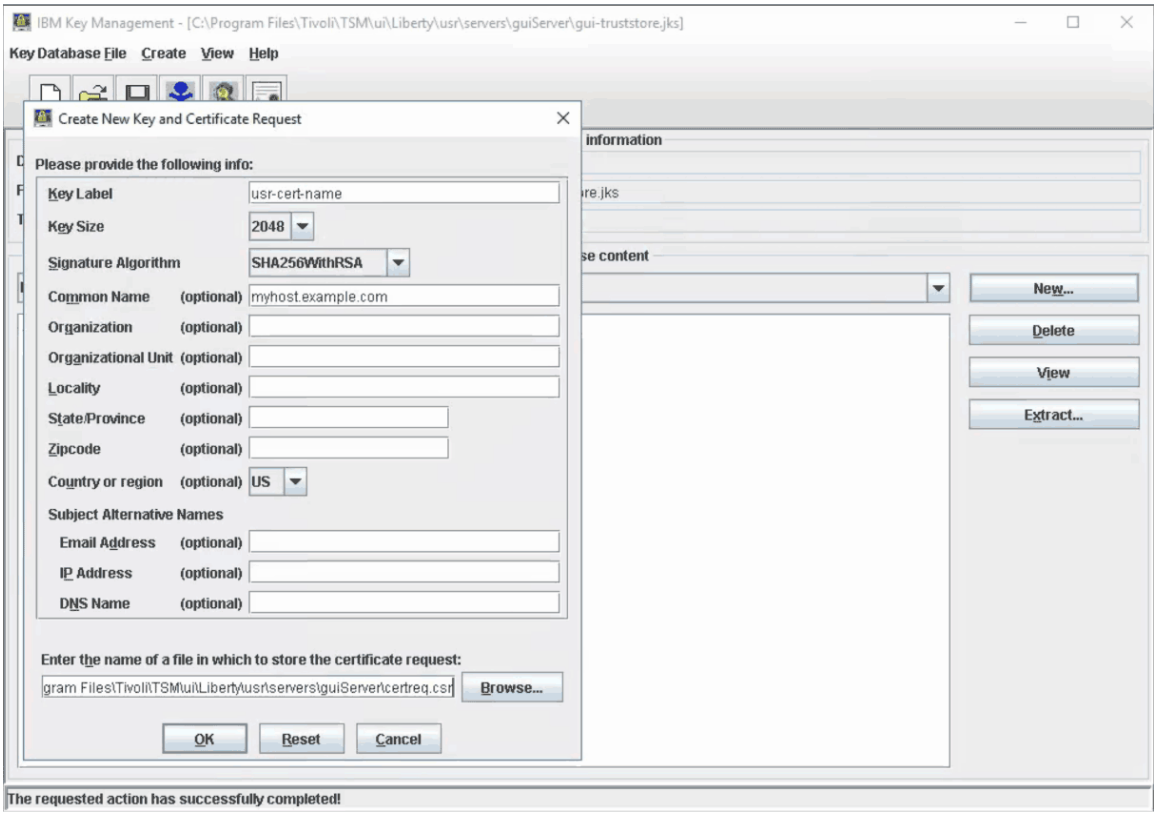
Schlüsselgröße
Wählen Sie eine Schlüsselgröße von mindestens 2048 Bit aus.

Unterschriftsalgorithmus
Wählen Sie **SHA256WithRSA** aus.

Allgemeiner Name
Geben Sie den vollständig qualifizierten Domänennamen (FQDN) des Systems im Netz an, auf dem das Operations Center installiert ist.

Hinweis: Der vollständig qualifizierte Domänenname (FQDN) des Systems in Ihrem Netz wird in der URL für das Operations Center in Ihrem System verwendet. Die URL wird von einem Web-Browser für den Zugriff auf das Operations Center verwendet.

Den Namen der Datei eingeben, in der die Zertifikatanforderung gespeichert werden soll
Geben Sie eine Datei mit dem Namen `certreq.csr` im Verzeichnis `guiServer` an.



e. Schließen Sie das Fenster **Öffnen**.

- Geben Sie den folgenden Befehl aus, um eine Zertifikatsanforderung mithilfe des Befehls **ikeycmd** zu erstellen:

```
ikeycmd -certreq -create -db gui-truststore.jks -size 2048
-sig_alg SHA256WithRSA -dn "CN=myhost.example.com" -file certreq.csr -label usr-cert-name
-san_dnsname myhost.example.com,myhost
-san_ipaddr 192.0.2.1,192.0.2.2
```

Hierbei gilt Folgendes:

-dn "CN=*myhost.example.com*"
Gibt den definierten Namen an. Geben Sie den Namen als Zeichenfolge in Anführungszeichen ein, die die Spezifikation CN=*myhost.example.com* enthält. Dabei gibt *myhost.example.com* den vollständig qualifizierten Domänennamen (FQDN) des Systems im Netz an, auf dem das Operations Center installiert ist.

Hinweis: Der vollständig qualifizierte Domänenname (FQDN) des Systems in Ihrem Netz wird in der URL für das Operations Center in Ihrem System verwendet. Die URL wird von einem Web-Browser für den Zugriff auf das Operations Center verwendet.

-label *usr-cert-name*
Gibt einen eindeutigen Kennsatz *usr-cert-name* für das Zertifikat in der Truststore-Datei an.

-san_dnsname *myhost.example.com,myhost* (Optional)
Gibt die Namen des Domänennamensservers (DNS) des Systems an, auf dem das Operations Center installiert ist. Der Wert von `CN` und der Wert von `dnsname` sind normalerweise identisch.

-san_ipaddr *192.0.2.1,192.0.2.2* (Optional)
Gibt die IP-Adresse des Systems an, auf dem das Operations Center installiert ist.

Zertifikatssignieranforderung an die Zertifizierungsstelle senden

Nachdem Sie die Zertifikatsanforderungsdatei (`certreq.csr`) erstellt haben, müssen Sie sie zum Signieren an die Zertifizierungsstelle senden. Befolgen Sie die Anweisungen von der Zertifizierungsstelle.

Signiertes Zertifikat empfangen

Die Zertifizierungsstelle muss Ihnen die Zertifikatsdatei senden, die der Truststore-Datei hinzuzufügen ist.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um das signierte Zertifikat zu empfangen:

1. Wechseln Sie in der Befehlszeile zur Schlüsselspeicherposition:

   Installationsverzeichnis/ui/Liberty/usr/servers/guiServer
2. Kopieren Sie die Dateien, die Sie von der Zertifizierungsstelle empfangen haben, an diese Position. Diese Dateien umfassen das CA-Stammzertifikat, die CA-Zwischenzertifikate (falls vorhanden) und das signierte Zertifikat für das Operations Center.
3. Stoppen Sie den Web-Server des Operations Center wie in „Web-Server starten und stoppen" auf Seite 179 beschrieben.
4. Erstellen Sie eine Sicherungskopie des Operations Center-Truststores für den Fall, dass der ursprüngliche Truststore wieder benötigt wird. Der Operations Center-Truststore hat den Namen `gui-truststore.jks`.
5. Verwenden Sie einen der folgenden Befehle, um die Schritte für den Empfang des signierten Zertifikats auszuführen:
   - Befehl **ikeyman**: Führen Sie die Schritte in „Signiertes Zertifikat mit IBM Key Management empfangen" auf Seite 170 aus.
   - Befehl **ikeycmd**: Führen Sie die Schritte in „Signiertes Zertifikat mit ikeycmd empfangen" auf Seite 177 aus.

Signiertes Zertifikat mit IBM Key Management empfangen

Zum Verwalten der Zertifikatsschlüssel und zum Empfangen des signierten Zertifikats können Sie eine grafische Benutzerschnittstelle, das Tool IBM Key Management, verwenden.

Vorgehensweise

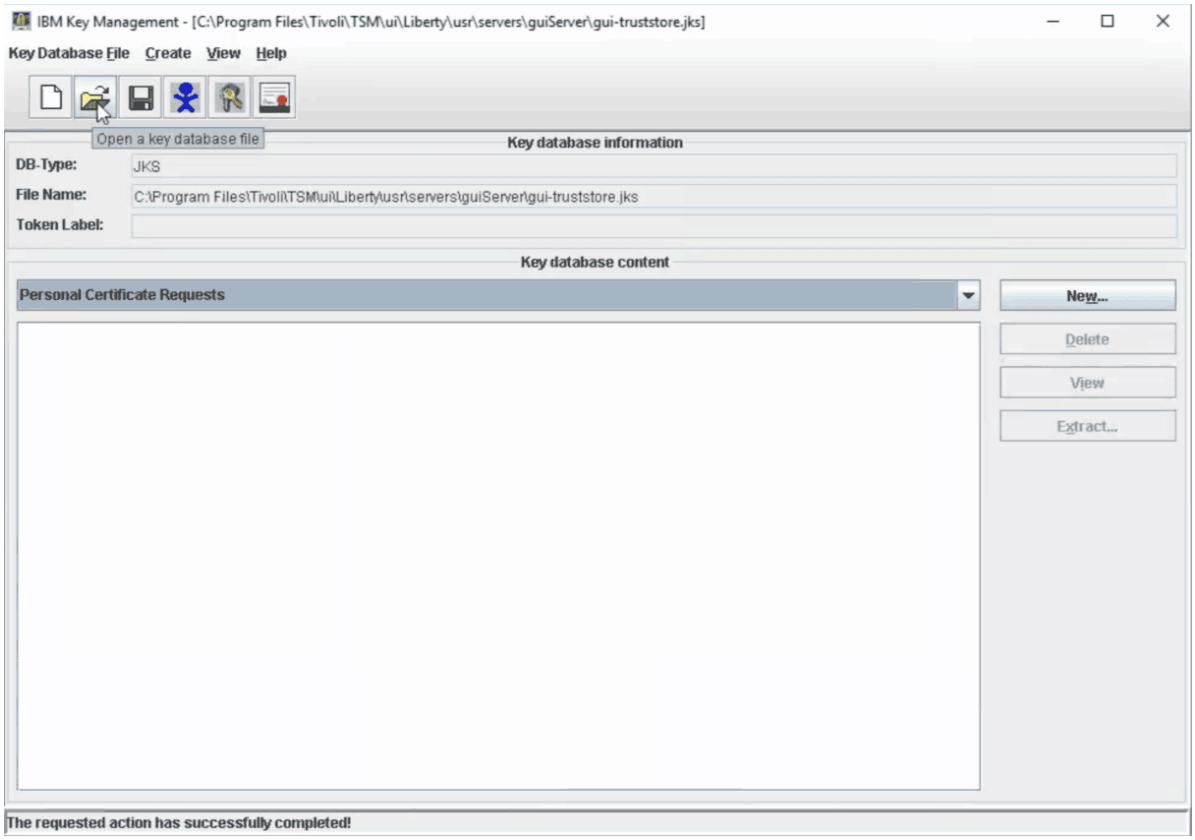
1. Überprüfen Sie mithilfe des Befehls **ikeyman**, ob sich das persönliche signierte Zertifikat im entsprechenden Verzeichnis befindet. Führen Sie die folgenden Schritte aus:
   a) Öffnen Sie das IBM Key Management-Tool, indem Sie den folgenden Befehl ausgeben:

   ```
   ikeyman
   ```

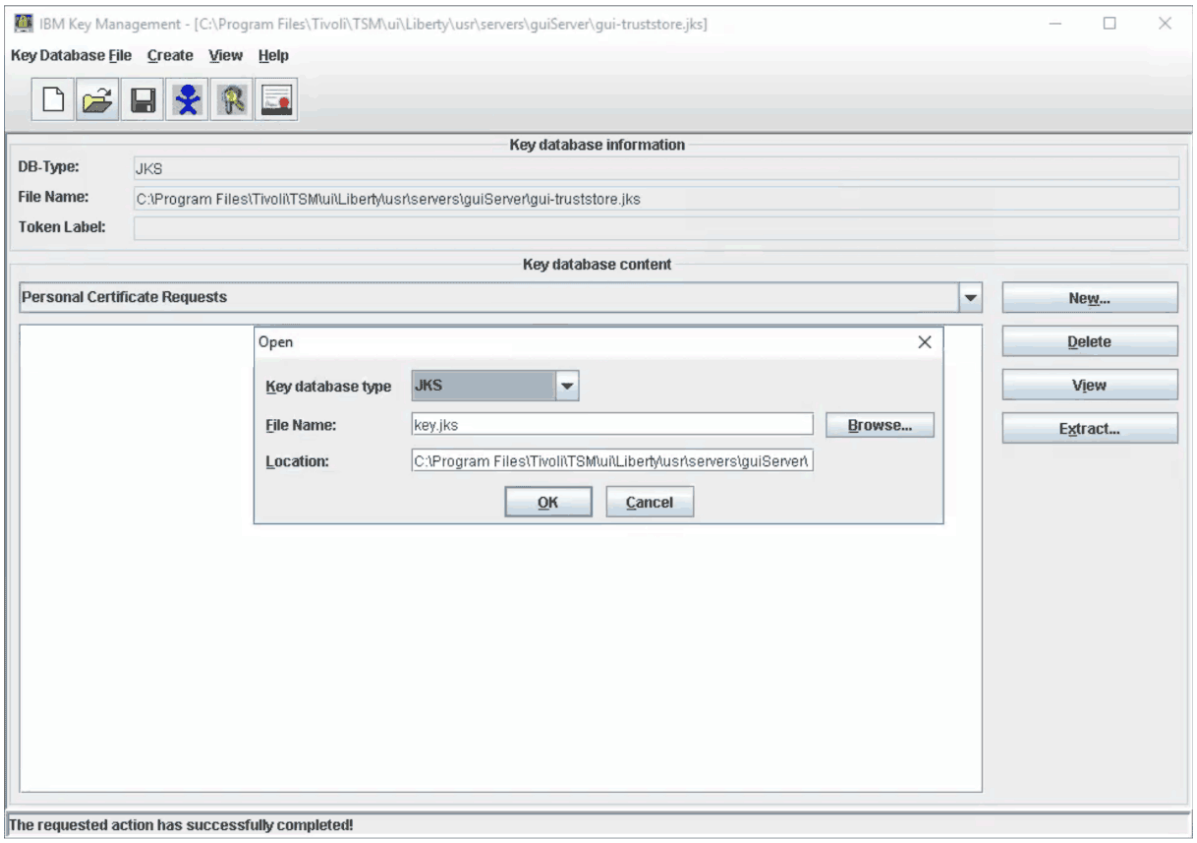
   Tipp: Sie müssen möglicherweise den vollständigen Pfad zum Befehl **ikeyman** angeben. Die Befehle befinden sich in dem folgenden Verzeichnis; dabei ist *Installationsverzeichnis* das Verzeichnis, in dem das Operations Center installiert ist:

   Installationsverzeichnis/ui/jre/bin

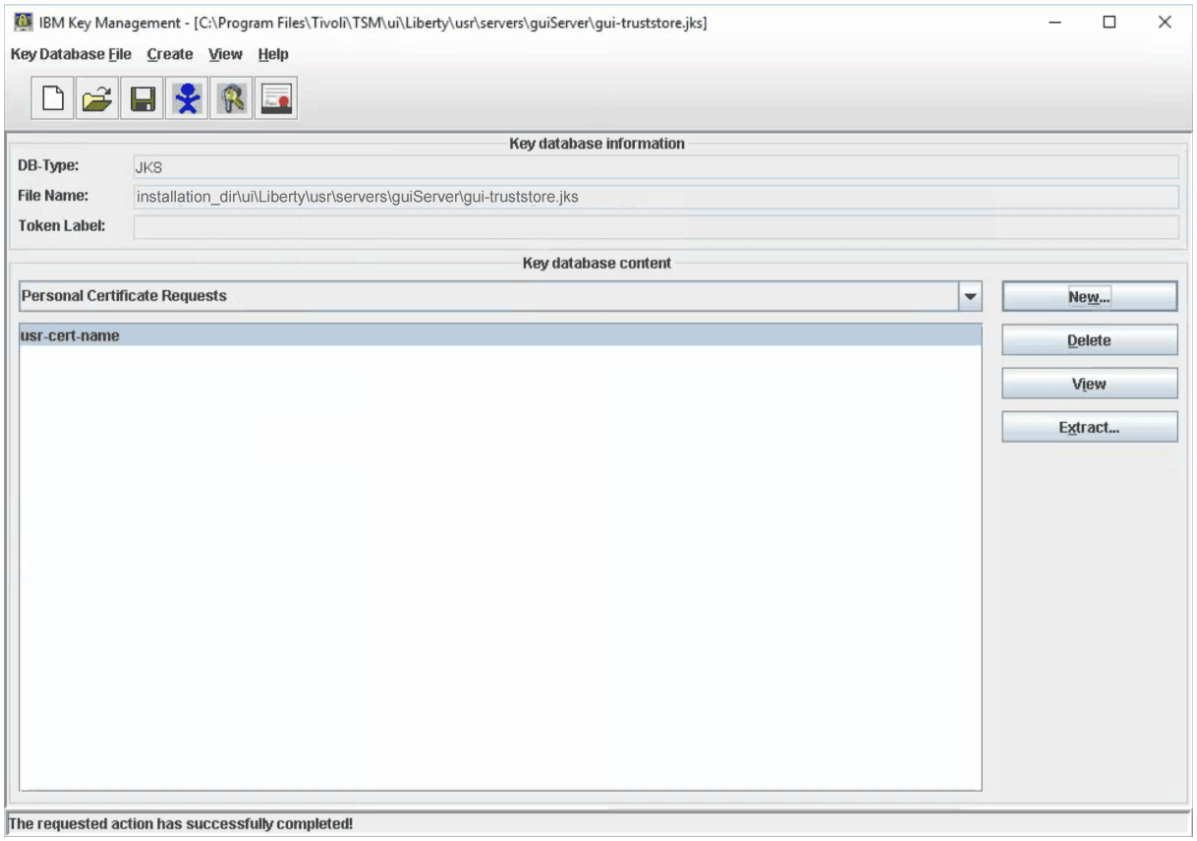
   b) Klicken Sie auf **Schlüsseldatenbankdatei** > **Öffnen**.



Klicken Sie im Dialogfenster **Öffnen** auf **Durchsuchen**, um das Verzeichnis zu öffnen, und wählen Sie die Datei `gui-truststore.jks` aus. Klicken Sie auf **OK**.



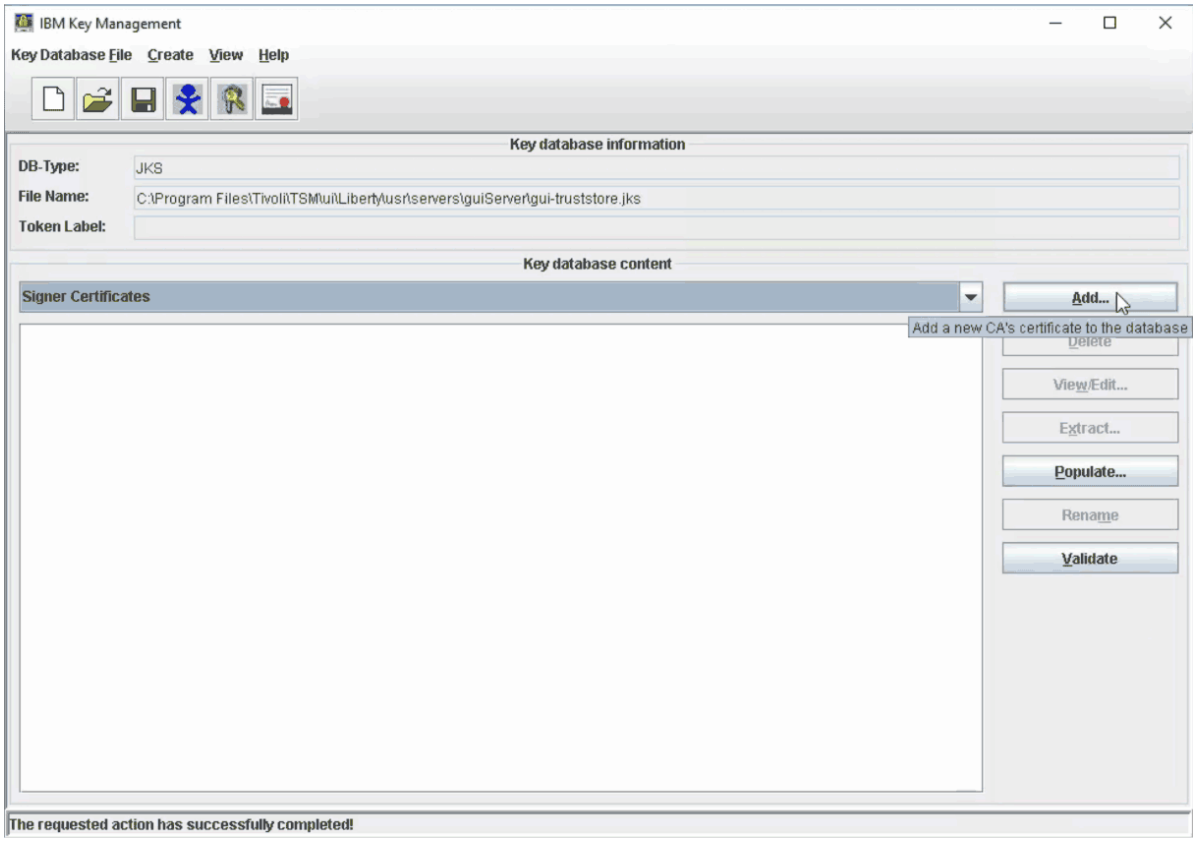
c) Wählen Sie **Persönliche Zertifikatsanforderungen** im Bereich **Schlüsseldatenbankinhalt** aus und bestätigen Sie, dass der Kennsatz **usr-cert-name** angezeigt wird.



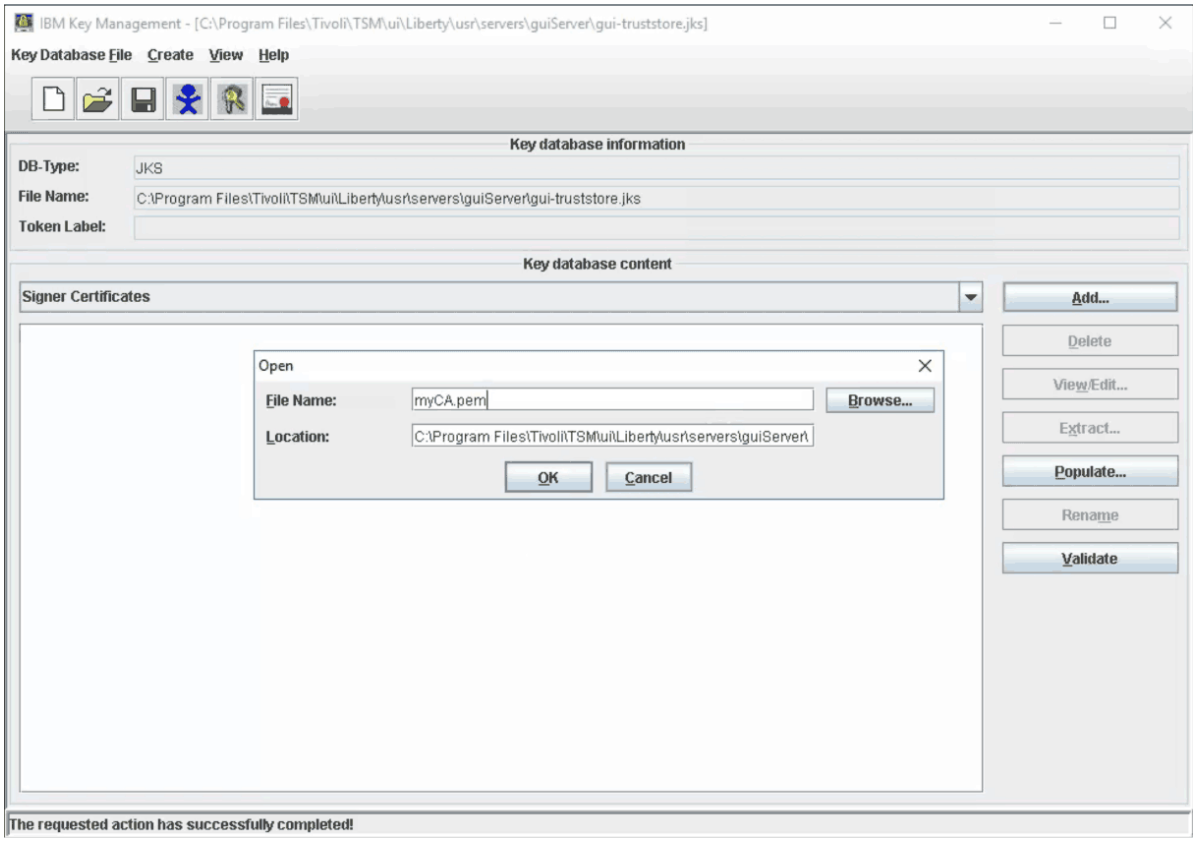
2. Fügen Sie der Truststore-Datei das CA-Stammzertifikat und alle Zwischenzertifikate hinzu. Wenn Sie Zwischenzertifikate von der Zertifizierungsstelle empfangen haben, müssen Sie jedes einzelne der Truststore-Datei hinzufügen, bevor Sie das CA-Stammzertifikat hinzufügen. Führen Sie die folgenden Schritte für jedes Zwischenzertifikat und das CA-Stammzertifikat aus.

   Wichtig: Die Zertifizierungsstelle sendet ein einziges Stammzertifikat, das signierte Zertifikat und möglicherweise mindestens ein Zwischenzertifikat. Je nach Zertifizierungsstelle kann die Zertifikatsdatei eine oder mehrere Dateien umfassen. Wenn Sie eine einzelne Zertifikatsdatei erhalten, müssen Sie die Zertifikate als separate Dateien extrahieren. Wenden Sie sich an Ihre Zertifizierungsstelle, wenn Sie beim Extrahieren der Zertifikate Unterstützung brauchen.

   a) Wählen Sie **Zertifikate des Unterzeichners** im Bereich **Schlüsseldatenbankinhalt** aus und klicken Sie auf **Hinzufügen**.

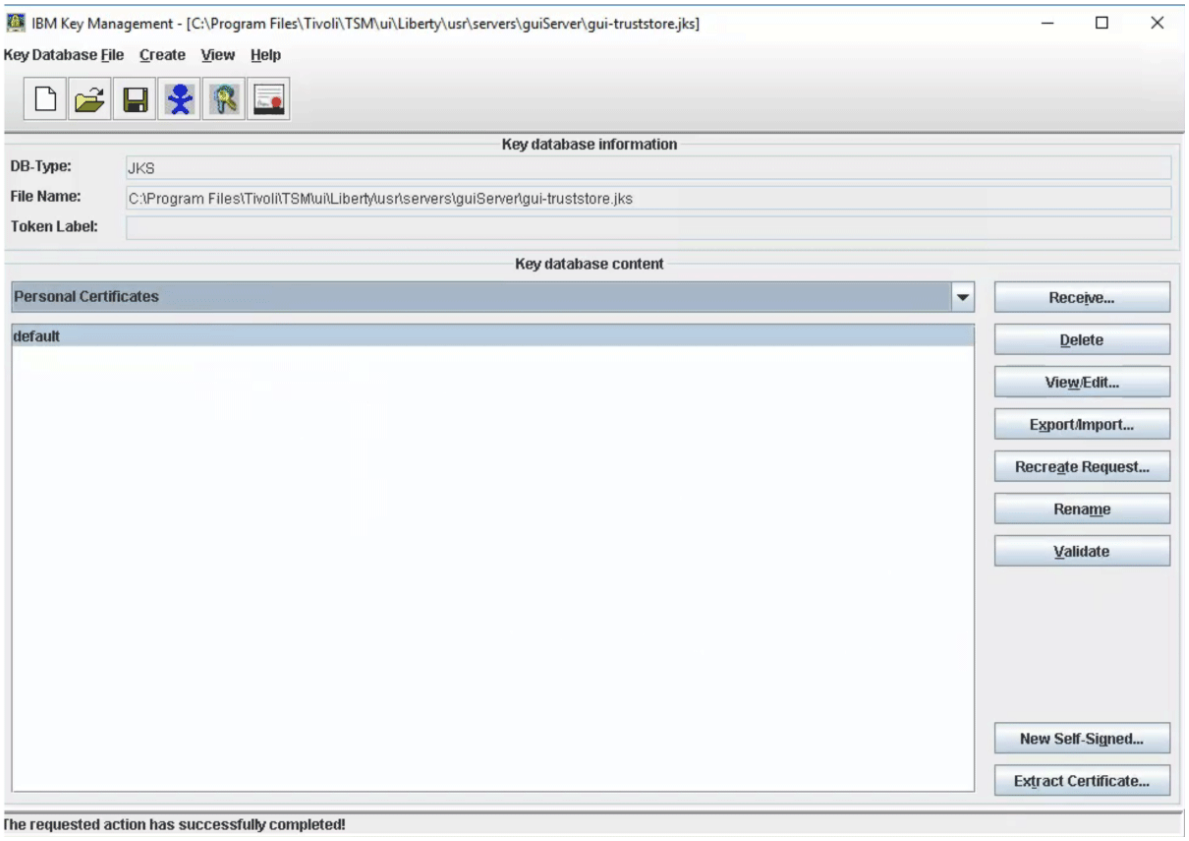


b) Geben Sie im Dialogfenster 'Öffnen' das CA-Stammzertifikat oder das Zwischenzertifikat an und klicken Sie auf **OK**.

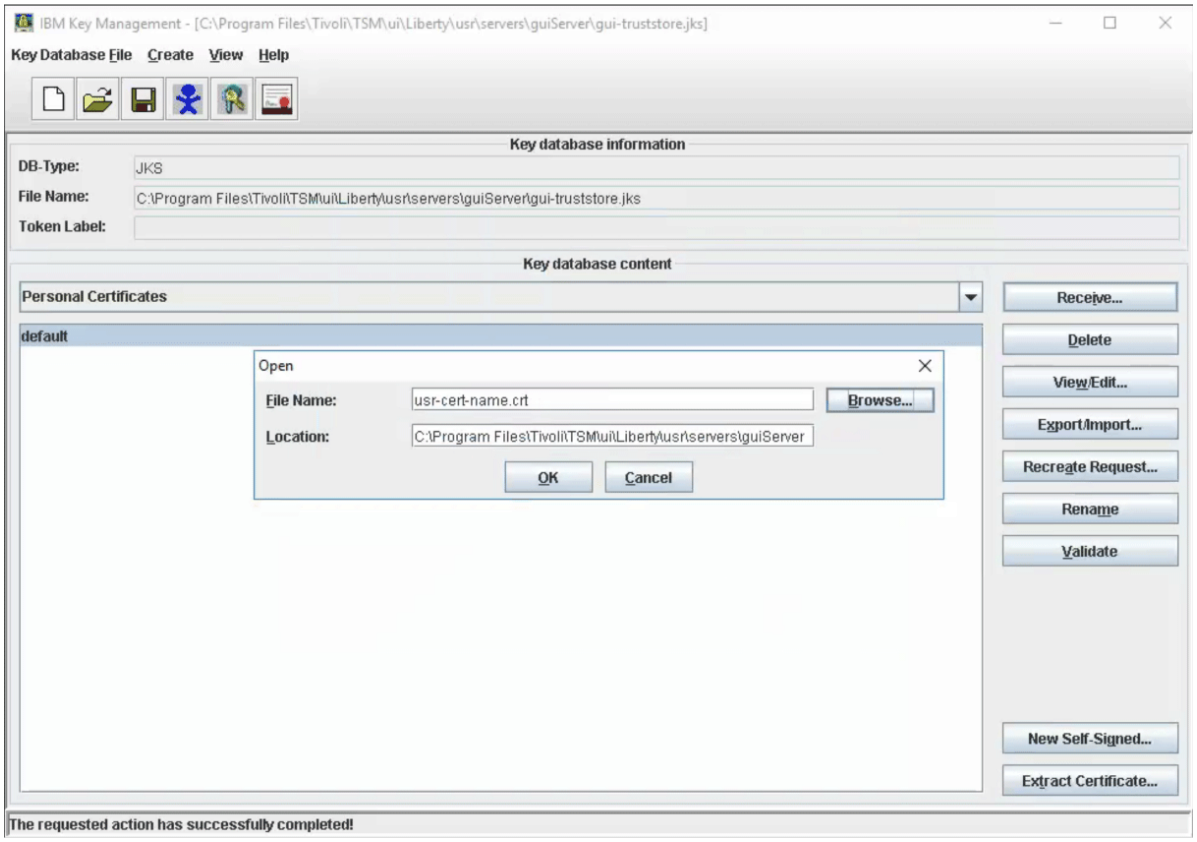


3. Führen Sie die folgenden Schritte aus, um das signierte Zertifikat zu empfangen:

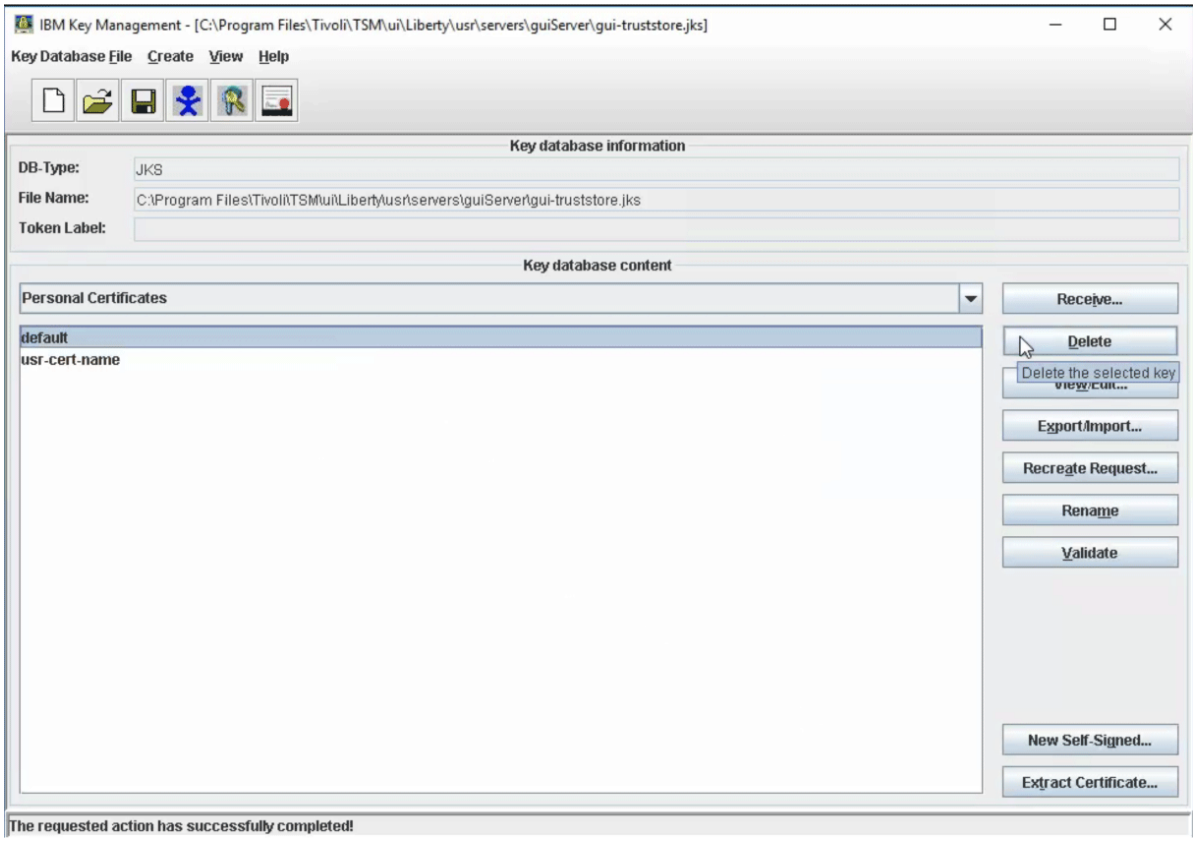
a) Wählen Sie **Persönliche Zertifikate** im Bereich **Schlüsseldatenbankinhalt** aus und klicken Sie auf **Empfangen**.



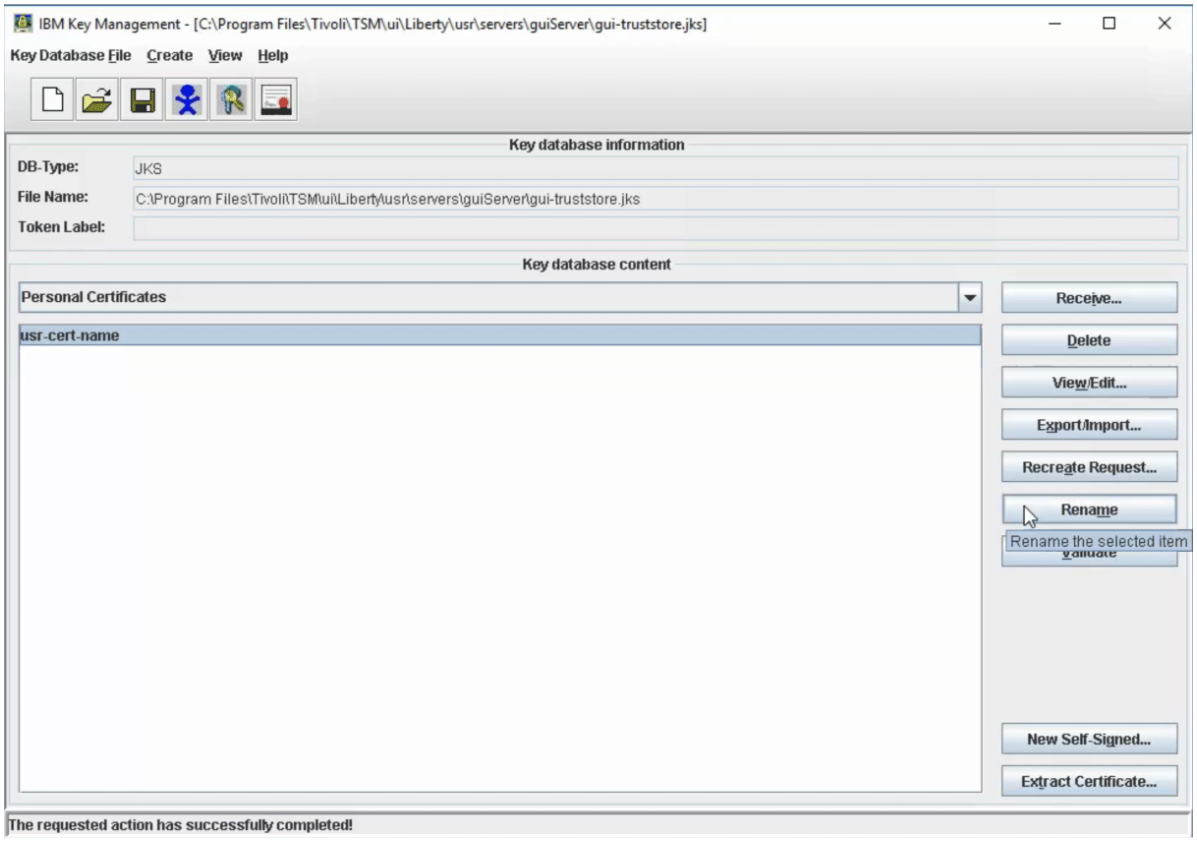
b) Geben Sie im Dialogfenster 'Öffnen' das signierte Zertifikat an und klicken Sie auf **OK**.



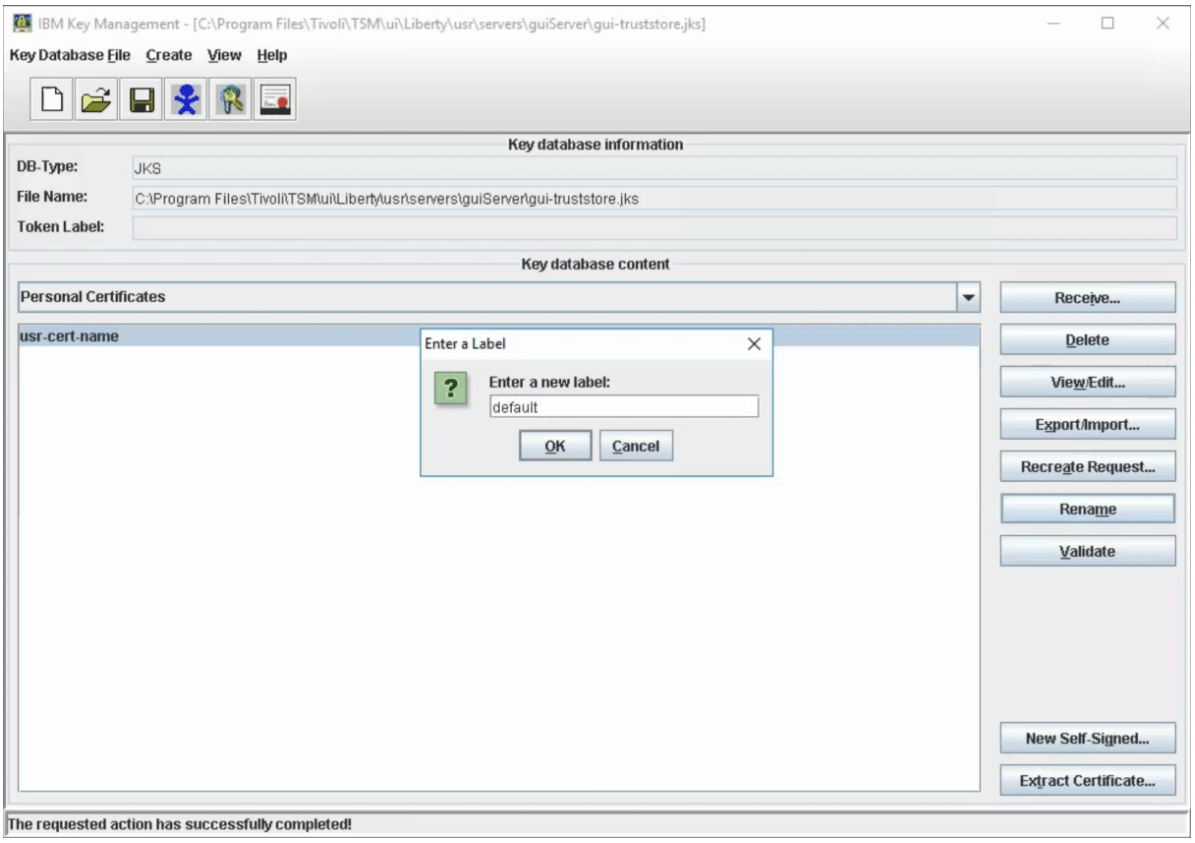
4. Löschen Sie das selbst signierte Zertifikat, das derzeit vom Operations Center verwendet wird, und ersetzen Sie es durch das von der Zertifizierungsstelle signierte Zertifikat. Gehen Sie wie folgt vor:
   a) Wählen Sie **Persönliche Zertifikate** im Bereich **Schlüsseldatenbankinhalt** aus.
   b) Wählen Sie das Zertifikat mit dem Kennsatz **default** aus und klicken Sie auf **Löschen**. Klicken Sie im Bestätigungsdialogfenster auf **Ja**.



   c) Wählen Sie das von der Zertifizierungsstelle signierte Zertifikat **usr-cert-name** aus und klicken Sie auf **Umbenennen**.



d) Benennen Sie im Dialogfenster 'Umbenennen' das signierte Zertifikat (`usr-cert-name`) in `default` um und klicken Sie auf **OK**.



5. Führen Sie die folgenden Schritte aus, um das Zertifikat `default` zu validieren:
   a) Wählen Sie **Persönliche Zertifikate** im Bereich **Schlüsseldatenbankinhalt** aus.

b) Wählen Sie das Zertifikat mit dem Kennsatz **default** aus und klicken Sie auf **Validieren**. Klicken Sie im Bestätigungsdialogfenster auf **OK**.

6. Starten Sie den Web-Server des Operations Center wie in „Web-Server starten und stoppen" auf Seite 179 beschrieben.

Signiertes Zertifikat mit `ikeycmd` empfangen

Der Befehl **`ikeycmd`**, mit dem eine Befehlszeile geöffnet wird, kann zum Verwalten von Zertifikatsschlüsseln und zum Empfangen signierter Zertifikate verwendet werden.

Vorgehensweise

1. Überprüfen Sie mithilfe des Befehls **`ikeycmd`**, ob sich das persönliche signierte Zertifikat im entsprechenden Verzeichnis befindet. Führen Sie die folgenden Schritte aus:

   a) Geben Sie den folgenden Befehl aus:

   ```
   ikeycmd -certreq -list -db gui-truststore.jks
   ```

   Tipp: Sie müssen möglicherweise den vollständigen Pfad zum Befehl **`ikeycmd`** angeben. Die Befehle befinden sich in dem folgenden Verzeichnis; dabei ist *Installationsverzeichnis* das Verzeichnis, in dem das Operations Center installiert ist:

   Installationsverzeichnis`/ui/jre/bin`

   b) In einer Nachricht wird der Name des persönlichen signierten Zertifikats, `usr-cert-name`, das sich in der Truststore-Datei befindet, angezeigt.

2. Fügen Sie der Truststore-Datei das CA-Stammzertifikat und alle Zwischenzertifikate hinzu, indem Sie die folgenden Befehle ausgeben. Wenn Sie Zwischenzertifikate von der Zertifizierungsstelle empfangen haben, müssen Sie diese der Truststore-Datei hinzufügen, bevor Sie das CA-Stammzertifikat hinzufügen.

   ```
   ikeycmd -cert -add -db gui-truststore.jks
       -file Zwischenzertifikatsdatei
   ```

   ```
   ikeycmd -cert -add -db gui-truststore.jks
       -file Stammzertifikatsdatei
   ```

   Hierbei gilt Folgendes:

   -file *Zertifikatsdatei*
   Gibt den Namen der Datei an, die das Zertifikat enthält.

3. Geben Sie den folgenden Befehl aus, um das signierte Zertifikat zu empfangen:

   ```
   ikeycmd -cert -receive -db gui-truststore.jks
   -file Unterzeichnerzertifikatsdatei
   ```

   Hierbei gilt Folgendes:

   -file *Unterzeichnerzertifikatsdatei*
   Gibt den Namen der Datei an, die das signierte Zertifikat enthält.

4. Löschen Sie das selbst signierte Zertifikat, das derzeit vom Operations Center verwendet wird, und ersetzen Sie es durch das von der Zertifizierungsstelle signierte Zertifikat. Gehen Sie wie folgt vor:

   a) Geben Sie den folgenden Befehl aus, um das vorhandene selbst signierte Zertifikat zu löschen:

   ```
   ikeycmd -cert -delete -db gui-truststore.jks -label default
   ```

   b) Geben Sie den folgenden Befehl aus, um das von der Zertifizierungsstelle signierte Zertifikat (*usr-cert-name*) in `default` umzubenennen:

   ```
   ikeycmd -cert -rename -db gui-truststore.jks -label usr-cert-name
   -new_label default
   ```

Hierbei gilt Folgendes:

-label *usr-cert-name*
Identifiziert das von der Zertifizierungsstelle signierte Zertifikat durch seinen Kennsatz.

5. Geben Sie den folgenden Befehl aus, um das Zertifikat `default` zu validieren:

```
ikeycmd -cert -validate -db gui-truststore.jks -label default
```

6. Befolgen Sie die Anweisungen in „Web-Server starten und stoppen” auf Seite 179, um den Web-Server des Operations Center zu starten.

Kennwort für die Truststore-Datei des Operations Center löschen und neu zuordnen

Um die sichere Kommunikation zwischen dem Operations Center und dem Hub-Server einrichten zu können, müssen Sie das Kennwort für die Truststore-Datei des Operations Center kennen. Sie erstellen dieses Kennwort während der Installation des Operations Center. Wenn Sie das Kennwort nicht kennen, können Sie es löschen und ein neues Kennwort zuordnen.

Informationen zu diesem Vorgang

Um ein neues Kennwort zuzuordnen, müssen Sie ein Kennwort erstellen, die Truststore-Datei des Operations Center löschen und den Web-Server des Operations Center erneut starten.

Achtung:

Wenn Sie das Truststore-Kennwort vergessen haben, müssen Sie ein neues signiertes Zertifikat von der Zertifizierungsstelle abrufen. Weitere Informationen finden Sie in „Signiertes Zertifikat empfangen” auf Seite 170.

Führen Sie die folgenden Schritte nur aus, wenn das Truststore-Kennwort nicht bekannt ist. Führen Sie diese Schritte nicht aus, wenn das Truststore-Kennwort bekannt ist und lediglich geändert werden soll. Um das Kennwort zu löschen und neu zuzuordnen, müssen Sie die Truststore-Datei löschen. Damit werden alle in der Truststore-Datei gespeicherten Zertifikate gelöscht. Wenn Sie das Truststore-Kennwort kennen, können Sie es mit dem Dienstprogramm **ikeycmd** oder **ikeyman** ändern.

Vorgehensweise

1. Stoppen Sie den Web-Server des Operations Center.
2. Wechseln Sie in das folgende Verzeichnis (*Installationsverzeichnis* ist das Verzeichnis, in dem das Operations Center installiert ist):

   Installationsverzeichnis/ui/Liberty/usr/servers/guiServer
3. Öffnen Sie die Datei `bootstrap.properties`, die das Kennwort für die Truststore-Datei enthält.

   Wenn das Kennwort nicht verschlüsselt ist, können Sie damit die Truststore-Datei öffnen, ohne es neu zuordnen zu müssen.

   Die folgenden Beispiele zeigen den Unterschied zwischen einem verschlüsselten und einem nicht verschlüsselten Kennwort:

   Beispiel eines verschlüsselten Kennworts
   Verschlüsselte Kennwörter beginnen mit der Zeichenfolge `{xor}`.

   Das folgende Beispiel zeigt ein verschlüsseltes Kennwort als Wert des Parameters **tsm.truststore.pswd**:

```
tsm.truststore.pswd={xor}MiYPPiwsKDAtOw==
```

Beispiel eines nicht verschlüsselten Kennworts
Das folgende Beispiel zeigt ein nicht verschlüsseltes Kennwort als Wert des Parameters **tsm.truststore.pswd**:

```
tsm.truststore.pswd=J8b%^B
```

4. Ersetzen Sie das Kennwort in der Datei `bootstrap.properties` durch ein neues Kennwort.
   Sie können das Kennwort durch ein verschlüsseltes Kennwort oder durch ein nicht verschlüsseltes Kennwort ersetzen. Merken Sie sich das nicht verschlüsselte Kennwort für eine spätere Verwendung.

   Gehen Sie wie folgt vor, um ein verschlüsseltes Kennwort zu erstellen:

   a. Erstellen Sie ein nicht verschlüsseltes Kennwort.

      Das Kennwort für die Truststore-Datei muss die folgenden Kriterien erfüllen:

      - Das Kennwort darf mindestens 6 Zeichen und maximal 64 Zeichen enthalten.
      - Das Kennwort muss mindestens die folgenden Zeichen enthalten:
        - Einen Großbuchstaben (A – Z)
        - Einen Kleinbuchstaben (a – z)
        - Eine Ziffer (0 – 9)
        - Zwei der nachfolgend aufgelisteten nicht alphanumerischen Zeichen:

          ```
          ~ @ # $ % ^ & * _ - + = ` |
          ```

          ```
          ( ) { } [ ] : ; < > , . ? /
          ```

   b. Wechseln Sie über die Befehlszeile des Betriebssystems in das folgende Verzeichnis:

      Installationsverzeichnis`/ui/Liberty/bin`

   c. Geben Sie den folgenden Befehl aus, um das Kennwort zu verschlüsseln (*mein_Kennwort* ist das nicht verschlüsselte Kennwort):

      `securityUtility encode` *mein_Kennwort* `--encoding=aes`

5. Speichern Sie die Datei `bootstrap.properties`.
6. Wechseln Sie in das folgende Verzeichnis:

   Installationsverzeichnis`/ui/Liberty/usr/servers/guiServer`

7. Löschen Sie die Truststore-Datei `gui-truststore.jks` des Operations Center.
8. Starten Sie den Web-Server des Operations Center.

   Informationen zum Starten des Web-Servers des Operations Center finden Sie in „Web-Server starten und stoppen" auf Seite 179.

Ergebnisse

Eine neue Truststore-Datei wird automatisch für das Operations Center erstellt und das TLS-Zertifikat des Operations Center wird automatisch in die Truststore-Datei eingefügt.

Web-Server starten und stoppen

Der Web-Server des Operations Center wird als Dienst ausgeführt und automatisch gestartet. Das Stoppen und Starten des Web-Servers kann z. B. für Konfigurationsänderungen erforderlich sein.

Vorgehensweise

Stoppen Sie den Web-Server und starten Sie ihn erneut.

- Wenn auf dem System **systemctl** installiert ist, geben Sie die folgenden Befehle aus:
  - Zum Stoppen des Servers:

```
systemctl stop opscenter.service
```

– Zum Starten des Servers:

```
systemctl start opscenter.service
```

– Zum erneuten Starten des Servers:

```
systemctl restart opscenter.service
```

– Geben Sie den folgenden Befehl aus, um festzustellen, ob der Server ausgeführt wird:

```
systemctl status opscenter.service
```

- Wenn auf dem System **systemctl** nicht installiert ist, geben Sie die folgenden Befehle aus:
  – Zum Stoppen des Servers:

```
service opscenter.rc stop
```

  – Zum Starten des Servers:

```
service opscenter.rc start
```

  – Zum erneuten Starten des Servers:

```
service opscenter.rc restart
```

  – Geben Sie den folgenden Befehl aus, um festzustellen, ob der Server ausgeführt wird:

```
service opscenter.rc status
```

Operations Center öffnen

Die Seite '**Übersicht**' ist die Standardeingangssicht im Operations Center. In Ihrem Web-Browser können Sie jedoch für die Seite, die bei der Anmeldung beim Operations Center geöffnet werden soll, ein Lesezeichen setzen.

Vorgehensweise

1. Geben Sie die folgende Adresse in einem Web-Browser an. Dabei steht *Hostname* für den Namen des Computers, auf dem das Operations Center installiert ist, und *sicherer_Anschluss* für die Anschlussnummer, die das Operations Center für die HTTPS-Kommunikation auf diesem Computer verwendet:

   ```
   https://Hostname:sicherer_Anschluss/oc
   ```

   Tipps:

   - Bei der URL muss die Groß-/Kleinschreibung beachtet werden. Achten Sie beispielsweise darauf, dass Sie "oc" wie gezeigt in Kleinbuchstaben eingeben.
   - Die Standardanschlussnummer für HTTPS-Kommunikation lautet 11090. Während der Installation des Operations Center kann jedoch eine andere Anschlussnummer im Bereich von 1024 bis 65535 angegeben werden. Nach der Installation kann ein Administrator im Operations Center die Verwendung des sicheren TCP/IP-Standardanschlusses (443) für die HTTPS-Kommunikation konfigurieren. Wenn im Operations Center die Verwendung von Anschluss 443 konfiguriert ist, müssen Sie beim Öffnen des Operations Center die Nummer des sicheren Anschlusses nicht angeben. Stattdessen geben Sie die folgende Adresse in einem an. Dabei steht *Hostname* für den Namen des Computers, auf dem das Operations Center installiert ist.

     ```
     https:Hostname/oc/
     ```

Weitere Informationen zur Konfiguration von Anschluss 443 für das Operations Center finden Sie in „Verwendung des sicheren TCP/IP-Standardanschlusses im Operations Center konfigurieren" auf Seite 158.

2. Melden Sie sich unter Verwendung einer Administrator-ID an, die auf dem Hub-Server registriert ist.

   Auf der Seite '**Übersicht**' können Sie Übersichtsdaten für Clients, Services, Server, Speicherpools und Speichereinheiten anzeigen. Sie können weitere Details anzeigen, indem Sie auf die Elemente klicken oder indem Sie die Menüleiste des Operations Center verwenden.

   Überwachung über eine mobile Einheit: Um die Speicherumgebung über Fernzugriff zu überwachen, können Sie die Seite '**Übersicht**' des Operations Center im Web-Browser einer mobilen Einheit anzeigen. Das Operations Center unterstützt den Apple Safari-Web-Browser auf dem iPad. Es können auch andere mobile Einheiten verwendet werden.

Diagnoseinformationen mit IBM Spectrum Protect-Clientverwaltungsservices erfassen

Der Clientverwaltungsservice erfasst Diagnoseinformationen über Clients für Sichern/Archivieren und stellt diese Informationen dem Operations Center für Basisüberwachungsfunktionen zur Verfügung.

Informationen zu diesem Vorgang

Nach der Installation des Clientverwaltungsservice können Sie die Diagnoseseite im Operations Center aufrufen, um Fehlerbehebungsinformationen für Clients für Sichern/Archivieren anzuzeigen.

Tipp: Stellen Sie vor der Installation des Clientverwaltungsservice sicher, dass zwischen dem Client für Sichern/Archivieren und dem Server eine Verbindung besteht. Die vom Client verwendete Server-Truststore-Datei erhält das SSL-Zertifikat erst, wenn das Clientsystem mit dem Server verbunden ist (SSL = Secure Sockets Layer).

Diagnoseinformationen können nur von Linux- und Windows-Clients erfasst werden. Administratoren können jedoch die Diagnoseinformationen unter AIX, Linux oder Windows im Operations Center anzeigen.

Sie können den Clientverwaltungsservice auch auf Knoten mit Einheiten zum Versetzen von Daten für IBM Spectrum Protect for Virtual Environments: Data Protection for VMware installieren, um Diagnoseinformationen über die Einheiten zum Versetzen von Daten zu erfassen.

Tipp: In der Dokumentation für den Clientverwaltungsservice ist *Clientsystem* das System, in dem der Client für Sichern/Archivieren installiert ist.

Clientverwaltungsservice mit einem grafisch orientierten Assistenten installieren

Sie müssen den Clientverwaltungsservice auf den von Ihnen verwalteten Clientsystemen installieren, um Diagnoseinformationen über Clients für Sichern/Archivieren (z. B. Clientprotokolldateien) zu erfassen.

Vorbereitende Schritte

Lesen Sie den Abschnitt „Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices" auf Seite 141.

Informationen zu diesem Vorgang

Sie müssen den Clientverwaltungsservice auf demselben Computer wie den Client für Sichern/Archivieren installieren.

Vorgehensweise

1. Laden Sie das Installationspaket für den Clientverwaltungsservice von einer IBM Download-Site, z. B. IBM Passport Advantage oder IBM Fix Central, herunter. Suchen Sie nach einem Dateinamen, der etwa wie folgt lautet: *<Version>*-IBM-SPCMS-*<Betriebssystem>*.bin.

   Die folgende Tabelle enthält die Namen der Installationspakete.

Clientbetriebssystem	Installationspaketname
Linux x86 64-Bit	8.1.x.000-IBM-SPCMS-Linuxx64.bin
Windows 32-Bit	8.1.x.000-IBM-SPCMS-Windows32.exe
Windows 64-Bit	8.1.x.000-IBM-SPCMS-Windows64.exe

2. Erstellen Sie ein Verzeichnis auf dem Clientsystem, das Sie verwalten wollen, und kopieren Sie das Installationspaket dorthin.
3. Extrahieren Sie den Inhalt der Installationspaketdatei.
   - Gehen Sie in Linux-Clientsystemen wie folgt vor:
     a. Geben Sie den folgenden Befehl aus, um aus der Datei eine ausführbare Datei zu machen:

        ```
        chmod +x 8.1.x.000-IBM-SPCMS-Linuxx64.bin
        ```

     b. Geben Sie den folgenden Befehl aus:

        ```
        ./8.1.x.000-IBM-SPCMS-Linuxx64.bin
        ```

   - In Windows-Clientsystemen klicken Sie doppelt auf den Namen des Installationspakets in Windows Explorer.

   Tipp: Wenn Sie das Paket zuvor bereits installiert und deinstalliert haben, wählen Sie bei der Aufforderung, die vorhandenen Installationsdateien zu ersetzen, **Alle** aus.

4. Führen Sie die Installationsstapeldatei in dem Verzeichnis aus, in dem Sie die Installationsdateien und zugehörige Dateien extrahiert haben. Dies ist das Verzeichnis, das Sie in Schritt „2" auf Seite 182 erstellt haben.
   - Geben Sie auf Linux-Clientsystemen den folgenden Befehl aus:

     ```
     ./install.sh
     ```

   - In Windows-Clientsystemen klicken Sie doppelt auf **install.bat**.
5. Befolgen Sie die Anweisungen im Assistenten von IBM Installation Manager, um den Clientverwaltungsservice zu installieren.

   Ist IBM Installation Manager auf dem Clientsystem noch nicht installiert, müssen Sie sowohl **IBM Installation Manager** als auch **IBM Spectrum Protect-Clientverwaltungsservices** auswählen.

   Tipp: Sie können die Standardposition für das Verzeichnis für gemeinsam genutzte Ressourcen und für das Installationsverzeichnis von IBM Installation Manager übernehmen.

Nächste Schritte

Überprüfen Sie die Installation.

Clientverwaltungsservice im unbeaufsichtigten Modus installieren

Sie können den Clientverwaltungsservice im unbeaufsichtigten Modus installieren. Im unbeaufsichtigten Modus geben Sie die Installationswerte in einer Antwortdatei an und führen anschließend einen Installationsbefehl aus.

Vorbereitende Schritte

Lesen Sie den Abschnitt „Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices" auf Seite 141.

Extrahieren Sie das Installationspaket gemäß den Anweisungen in „Clientverwaltungsservice mit einem grafisch orientierten Assistenten installieren" auf Seite 181.

Informationen zu diesem Vorgang

Sie müssen den Clientverwaltungsservice auf demselben Computer wie den Client für Sichern/Archivieren installieren.

Das Verzeichnis `input`, das sich in dem Verzeichnis befindet, in dem das Installationspaket extrahiert wird, enthält die folgende Musterantwortdatei:

`install_response_sample.xml`

Sie können die Musterdatei mit den Standardwerten verwenden oder diese Datei anpassen.

Tipp: Wenn Sie die Musterdatei anpassen wollen, müssen Sie eine Kopie der Musterdatei erstellen, die Kopie umbenennen und bearbeiten.

Vorgehensweise

1. Erstellen Sie eine auf der Musterdatei basierende Antwortdatei oder verwenden Sie die Musterdatei `install_response_sample.xml`.

   In beiden Fällen müssen Sie sicherstellen, dass in der Antwortdatei die Anschlussnummer für den Clientverwaltungsservice angegeben ist. Der Standardanschluss ist 9028. Beispiel:

   ```
   <variable name='port' value='9028'/>
   ```

2. Führen Sie den Installationsbefehl für den Clientverwaltungsservice aus und akzeptieren Sie die Lizenz. Geben Sie in dem Verzeichnis, in dem die Installationspaketdatei extrahiert wurde, den folgenden Befehl aus (*Antwordatei* steht für den Pfad der Antwortdatei einschließlich des Dateinamens):

   Auf einem Linux-Clientsystem:

   ```
   ./install.sh -s -input Antwortdatei -acceptLicense
   ```

   Beispiel:

   ```
   ./install.sh -s -input /cms_install/input/install_response.xml -acceptLicense
   ```

   Auf einem Windows-Clientsystem:

   ```
   install.bat -s -input Antwortdatei -acceptLicense
   ```

   Beispiel:

   ```
   install.bat -s -input c:\cms_install\input\install_response.xml -acceptLicense
   ```

Nächste Schritte

Überprüfen Sie die Installation.

Überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert wurde

Bevor Sie Diagnoseinformationen über einen Client für Sichern/Archivieren mit dem Clientverwaltungsservice erfassen, können Sie überprüfen, ob der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert wurde.

Vorgehensweise

Geben Sie auf dem Clientsystem die folgenden Befehle in die Befehlszeile ein, um die Konfiguration des Clientverwaltungsservice anzuzeigen:

- Geben Sie auf Linux-Clientsystemen den folgenden Befehl aus:

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

  Clientinstallationsverzeichnis ist das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie bei einer Standardclientinstallation beispielsweise den folgenden Befehl aus:

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

  Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

  ```
  CMS-Konfiguration auflisten

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

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

- Geben Sie auf Windows-Clientsystemen den folgenden Befehl aus:

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

  Clientinstallationsverzeichnis ist das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist. Geben Sie bei einer Standardclientinstallation beispielsweise den folgenden Befehl aus:

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

  Die Ausgabe kann wie in dem folgenden Beispiel aussehen:

  ```
  CMS-Konfiguration auflisten

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

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

Wenn der Clientverwaltungsservice ordnungsgemäß installiert und konfiguriert ist, zeigt die Ausgabe die Position der Fehlerprotokolldatei an.

Der Ausgabetext wird aus der folgenden Konfigurationsdatei extrahiert:

- Auf Linux-Clientsystemen:

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

- Auf Windows-Clientsystemen:

  ```
  Clientinstallationsverzeichnis\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
  ```

Wenn die Ausgabe keine Einträge enthält, müssen Sie die Datei `client-configuration.xml` konfigurieren. Anweisungen zur Konfiguration dieser Datei finden Sie in Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren. Mit dem Befehl **`CmsConfig verify`** können Sie überprüfen, ob eine Knotendefinition in der Datei `client-configuration.xml` ordnungsgemäß erstellt wurde.

Operations Center für die Verwendung des Clientverwaltungsservice konfigurieren

Wenn Sie nicht die Standardkonfiguration für den Clientverwaltungsservice verwenden, müssen Sie das Operations Center für den Zugriff auf den Clientverwaltungsservice konfigurieren.

Vorbereitende Schritte

Stellen Sie sicher, dass der Clientverwaltungsservice auf dem Clientsystem installiert und gestartet wird. Lesen Sie den Abschnitt „Voraussetzungen und Einschränkungen für IBM Spectrum Protect-Clientverwaltungsservices” auf Seite 141.

Überprüfen Sie, ob die Standardkonfiguration verwendet wird. Die Standardkonfiguration wird nicht verwendet, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Clientverwaltungsservice verwendet nicht die Standardanschlussnummer 9028.
- Für den Zugriff auf den Client für Sichern/Archivieren wird nicht dieselbe IP-Adresse wie für das Clientsystem verwendet, in dem der Client für Sichern/Archivieren installiert ist. Eine andere IP-Adresse könnte beispielsweise in den folgenden Situationen verwendet werden:
  - Das Computersystem verfügt über zwei Netzkarten. Der Client für Sichern/Archivieren ist für die Kommunikation in einem Netz konfiguriert, während der Clientverwaltungsservice in dem anderen Netz kommuniziert.
  - Das Clientsystem ist mit DHCP (Dynamic Host Configuration Protocol) konfiguiert. Folglich wird dem Clientsystem eine IP-Adresse dynamisch zugeordnet, die während der vorherigen Operation des Clients für Sichern/Archivieren auf dem IBM Spectrum Protect-Server gespeichert wird. Wenn das Clientsystem neu gestartet wird, kann ihm eine andere IP-Adresse zugeordnet werden. Um sicherzustellen, dass das Operations Center das Clientsystem immer finden kann, geben Sie einen vollständig qualifizierten Domänennamen an.

Vorgehensweise

Gehen Sie wie folgt vor, um das Operations Center für die Verwendung des Clientverwaltungsservice zu konfigurieren:

1. Wählen Sie auf der Seite **Clients** des Operations Center den Client aus.
2. Klicken Sie auf **Details**.
3. Klicken Sie auf die Registerkarte **Eigenschaften**.
4. Geben Sie im Feld **URL für Ferndiagnose** im Abschnitt **Allgemein** die URL für den Clientverwaltungsservice im Clientsystem an.

   Die Adresse muss mit `https` beginnen. Die folgende Tabelle enthält Beispiele der URL für Ferndiagnose.

URL-Typ	Beispiel
Mit DNS-Hostnamen und Standardanschluss 9028	`https://server.example.com`
Mit DNS-Hostnamen und ohne Standardanschluss	`https://server.example.com:1599`
Mit IP-Adresse und ohne Standardanschluss	`https://192.0.2.0:1599`

5. Klicken Sie auf **Speichern**.

Nächste Schritte

Auf Clientdiagnoseinformationen (z. B. Clientprotokolldateien) können Sie über die Registerkarte **Diagnose** im Operations Center zugreifen.

Clientverwaltungsservice starten und stoppen

Der Clientverwaltungsservice wird nach seiner Installation auf dem Clientsystem automatisch gestartet. Sie müssen den Service in bestimmten Situationen möglicherweise stoppen und starten.

Prozedur

- Geben Sie die folgenden Befehle aus, um den Clientverwaltungsservice auf Linux-Clientsystemen zu stoppen, zu starten oder erneut zu starten:
  - Wenn auf dem System **systemctl** installiert ist, geben Sie die folgenden Befehle aus:
    - Zum Stoppen des Servers:

      ```
      systemctl stop cms.service
      ```

    - Zum Starten des Servers:

      ```
      systemctl start cms.service
      ```

    - Zum erneuten Starten des Servers:

      ```
      systemctl restart cms.service
      ```

    - Geben Sie den folgenden Befehl aus, um festzustellen, ob der Server ausgeführt wird:

      ```
      systemctl status cms.service
      ```

  - Wenn auf dem System **systemctl** nicht installiert ist, geben Sie die folgenden Befehle aus:
    - Zum Stoppen des Servers:

      ```
      service cms.rc stop
      ```

    - Zum Starten des Servers:

      ```
      service cms.rc start
      ```

    - Zum erneuten Starten des Servers:

      ```
      service cms.rc restart
      ```

    - Geben Sie den folgenden Befehl aus, um festzustellen, ob der Server ausgeführt wird:

      ```
      service cms.rc status
      ```

- Auf Windows-Clientsystemen öffnen Sie das Fenster **Dienste**, wo Sie den Dienst 'IBM Spectrum Protect-Clientverwaltungsservices' stoppen, starten oder erneut starten können.

Clientverwaltungsservice deinstallieren

Wenn Sie keine Clientdiagnoseinformationen mehr erfassen müssen, können Sie den Clientverwaltungsservice im Clientsystem deinstallieren.

Informationen zu diesem Vorgang

Sie müssen den Clientverwaltungsservice mit IBM Installation Manager deinstallieren. Falls nicht mehr benötigt, können Sie auch IBM Installation Manager deinstallieren.

Vorgehensweise

1. Deinstallieren Sie den Clientverwaltungsservice wie folgt auf dem Clientsystem:
   a) Öffnen Sie IBM Installation Manager:

- Wechseln Sie im Linux-Clientsystem in dem Verzeichnis, in dem IBM Installation Manager installiert ist, in das Unterverzeichnis `eclipse` (z. B. `/opt/IBM/InstallationManager/eclipse`) und geben Sie folgenden Befehl aus:

  ```
  ./IBMIM
  ```

- Im Windows-Clientsystem öffnen Sie IBM Installation Manager über das Menü **Start**.

b) Klicken Sie auf **Deinstallieren**.

c) Wählen Sie **IBM Spectrum Protect-Clientverwaltungsservices** aus und klicken Sie auf **Weiter**.

d) Klicken Sie auf **Deinstallieren** und dann auf **Fertigstellen**.

e) Schließen Sie das **IBM Installation Manager**-Fenster.

2. Falls Sie IBM Installation Manager nicht mehr benötigen, deinstallieren Sie es im Clientsystem:

a) Öffnen Sie den Deinstallationsassistenten von IBM Installation Manager:

- Wechseln Sie im Linux-Clientsystem in das Deinstallationsverzeichnis von IBM Installation Manager (z. B. `/var/ibm/InstallationManager/uninstall`) und geben Sie den folgenden Befehl aus:

  ```
  ./uninstall
  ```

- Im Windows-Clientsystem klicken Sie auf **Start** > **Systemsteuerung**. Dann klicken Sie auf **Programm deinstallieren** > **IBM Installation Manager** > **Deinstallieren**.

b) Wählen Sie **IBM Installation Manager** im Fenster **IBM Installation Manager** aus (falls noch nicht ausgewählt) und klicken Sie auf **Weiter**.

c) Klicken Sie auf **Deinstallieren** und dann auf **Fertigstellen**.

Clientverwaltungsservice für angepasste Clientinstallationen konfigurieren

Der Clientverwaltungsservice verwendet Informationen in der Clientkonfigurationsdatei (`client-configuration.xml`), um Diagnoseinformationen zu erkennen. Wenn der Clientverwaltungsservice die Position der Protokolldateien nicht erkennen kann, müssen Sie das Dienstprogramm **CmsConfig** ausführen, um die Position der Protokolldateien zur Datei `client-configuration.xml` hinzuzufügen.

Informationen zu diesem Vorgang

Stellen Sie vor der Installation des Clientverwaltungsservice sicher, dass zwischen dem Client für Sichern/Archivieren und dem Server eine Verbindung besteht. Die vom Client verwendete Server-Truststore-Datei erhält das SSL-Zertifikat erst, wenn das Clientsystem mit dem Server verbunden ist (SSL = Secure Sockets Layer).

Dienstprogramm CmsConfig

Wenn Sie nicht die Standardclientkonfiguration verwenden, können Sie das Dienstprogramm **CmsConfig** auf dem Clientsystem ausführen, um die Position der Clientprotokolldateien zu erkennen und zur Datei `client-configuration.xml` hinzuzufügen. Nach Abschluss der Konfiguration kann der Clientverwaltungsservice auf die Clientprotokolldateien zugreifen und sie für Basisdiagnosefunktionen im Operations Center zur Verfügung stellen.

Mit dem Dienstprogramm **CmsConfig** können Sie außerdem die Konfiguration des Clientverwaltungsservice anzeigen und einen Knotennamen aus der Datei `client-configuration.xml` entfernen.

Die Datei `client-configuration.xml` befindet sich in folgendem Verzeichnis:

- Auf Linux-Clientsystemen:

  ```
  Clientinstallationsverzeichnis/cms/Liberty/usr/servers/cmsServer
  ```

- Auf Windows-Clientsystemen:

  ```
  Clientinstallationsverzeichnis\cms\Liberty\usr\servers\cmsServer
  ```

Clientinstallationsverzeichnis ist das Verzeichnis, in dem der Client für Sichern/Archivieren installiert ist.

Das Dienstprogramm **CmsConfig** steht an den folgenden Positionen zur Verfügung.

Clientbetriebssystem	Position und Name des Dienstprogramms
Linux	*Clientinstallationsverzeichnis*/cms/bin/CmsConfig.sh
Windows	*Clientinstallationsverzeichnis*\cms\bin\CmsConfig.bat

Für die Verwendung des Dienstprogramms **CmsConfig** geben Sie einen beliebigen der im Dienstprogramm enthaltenen Befehle aus. Sie müssen jeden Befehl in einer einzelnen Zeile eingeben.

Befehl CmsConfig discover

Mit dem Befehl **CmsConfig discover** können Sie Options- und Protokolldateien automatisch erkennen und der Clientkonfigurationsdatei `client-configuration.xml` hinzufügen. Auf diese Weise können Sie dafür sorgen, dass der Clientverwaltungsservice auf die Clientprotokolldateien zugreifen und sie für die Diagnose im Operations Center zur Verfügung stellen kann.

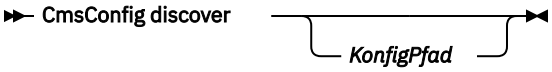
Normalerweise führt das Installationsprogramm des Clientverwaltungsservice den Befehl **CmsConfig discover** automatisch aus. Sie müssen diesen Befehl jedoch manuell ausführen, wenn Sie den Client für Sichern/Archivieren geändert haben (z. B. Client hinzugefügt) oder wenn Sie die Serverkonfiguration oder die Position der Protokolldateien geändert haben.

Damit der Clientverwaltungsservice eine Protokolldefinition in der Datei `client-configuration.xml` erstellt, müssen die Serveradresse, der Serveranschluss und der Clientknotenname von IBM Spectrum Protect abgerufen werden. Ist der Knotenname in der Clientoptionsdatei (normalerweise `dsm.sys` auf Linux-Clientsystemen und `dsm.opt` auf Windows-Clientsystemen) nicht definiert, wird der Hostname des Clientsystems verwendet.

Für eine Aktualisierung der Clientkonfigurationsdatei muss der Clientverwaltungsservice auf mindestens eine Protokolldatei zugreifen, z. B. `dsmerror.log` und `dsmsched.log`. Die besten Ergebnisse erzielen Sie, wenn Sie den Befehl **CmsConfig discover** in demselben Verzeichnis und unter Verwendung derselben Umgebungsvariablen wie für den Befehl des Clients für Sichern/Archivieren (**dsmc**) ausführen. Auf diese Weise können Sie die Chancen verbessern, die richtigen Protokolldateien zu finden.

Wenn sich die Clientoptionsdatei an einer benutzerdefinierten Position befindet oder keinen typischen Optionsdateinamen hat, können Sie auch den Pfad für die Clientoptionsdatei angeben, um den Bereich der Erkennung einzugrenzen.

Syntax



Parameter

KonfigPfad

Der Pfad der Clientoptionsdatei (normalerweise `dsm.opt`). Geben Sie den Konfigurationspfad an, wenn sich die Clientoptionsdatei nicht an der Standardposition befindet oder nicht den Standardnamen hat. Der Clientverwaltungsservice lädt die Clientoptionsdatei und erkennt die Clientknoten und -protokolle anhand dieser Datei. Dieser Parameter ist optional.

Auf einem Linux-Clientsystem lädt der Clientverwaltungsservice die Clientbenutzeroptionsdatei (`dsm.opt`) immer zuerst und sucht dann nach der Clientsystemoptionsdatei (normalerweise `dsm.sys`). Der Wert des Parameters *KonfigPfad* ist jedoch immer die Clientbenutzeroptionsdatei.

Beispiele für ein Linux-Clientsystem

- Die Clientprotokolldateien erkennen und die Protokolldefinitionen automatisch zur Datei `client-configuration.xml` hinzufügen.

  Geben Sie den folgenden Befehl im Verzeichnis `/opt/tivoli/tsm/cms/bin` aus.

  Befehl:
  ```
  ./CmsConfig.sh discover
  ```

  Ausgabe:

  ```
  Clientkonfiguration und Protokolle werden erkannt.

  server.example.com:1500 SUSAN
      /opt/tivoli/tsm/client/ba/bin/dsmerror.log

  Clientkonfigurations- und Protokollerkennung beendet.
  ```

- Die in der Datei `/opt/tivoli/tsm/client/ba/bin/daily.opt` angegebenen Konfigurations- und Protokolldateien erkennen und die Protokolldefinitionen automatisch zur Datei `client-configuration.xml` hinzufügen.

  Geben Sie den folgenden Befehl im Verzeichnis `/opt/tivoli/tsm/cms/bin` aus.

  Befehl:
  ```
  ./CmsConfig.sh discover /opt/tivoli/tsm/client/ba/bin/daily.opt
  ```

  Ausgabe:

  ```
  Clientkonfiguration und Protokolle werden erkannt

  server.example.com:1500 NO_SSL SUSAN
            Funktionen: [LOG_QUERY]
      Optionsdateipfad: /opt/tivoli/tsm/client/ba/bin/dsm.sys

        Protokolldatei: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
        Protokolldatei: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
          en_US MM/dd/yyyy HH:mm:ss Windows-1252
  Clientkonfigurations- und Protokollerkennung beendet.
  ```

Beispiele für ein Windows-Clientsystem

- Die Clientprotokolldateien erkennen und die Protokolldefinitionen automatisch zur Datei `client-configuration.xml` hinzufügen.

  Geben Sie den folgenden Befehl im Verzeichnis `C:\Programme\Tivoli\TSM\cms\bin` aus.

  Befehl:
  ```
  cmsconfig discover
  ```

  Ausgabe:

  ```
  Clientkonfiguration und Protokolle werden erkannt.

  server.example.com:1500 SUSAN
      C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
  Clientkonfigurations- und Protokollerkennung beendet.
  ```

- Die in der Datei `c:\program files\tivoli\tsm\baclient\daily.opt` angegebenen Konfigurations- und Protokolldateien erkennen und die Protokolldefinitionen automatisch zur Datei `client-configuration.xml` hinzufügen.

  Geben Sie den folgenden Befehl im Verzeichnis `C:\Programme\Tivoli\TSM\cms\bin` aus.

  Befehl:
  ```
  cmsconfig discover "c:\program files\tivoli\tsm\baclient\daily.opt"
  ```

Ausgabe:

```
Clientkonfiguration und Protokolle werden erkannt

server.example.com:1500 NO_SSL SUSAN
          Funktionen: [LOG_QUERY]
    Optionsdateipfad: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

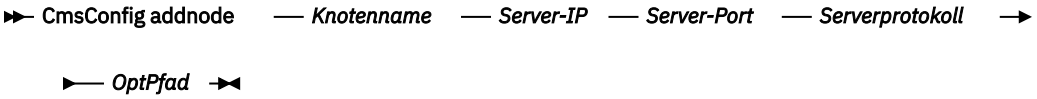
      Protokolldatei: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
      Protokolldatei: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log
        en_US MM/dd/yyyy HH:mm:ss Windows-1252
Clientkonfigurations- und Protokollerkennung beendet.
```

Befehl `CmsConfig addnode`

Mit dem Befehl **`CmsConfig addnode`** können Sie eine Clientknotendefinition in der Konfigurationsdatei `client-configuration.xml` manuell hinzufügen. Die Knotendefinition enthält Informationen, die der Clientverwaltungsservice für die Kommunikation mit dem IBM Spectrum Protect-Server benötigt.

Verwenden Sie diesen Befehl nur, wenn die Clientoptionsdatei oder die Clientprotokolldateien nicht an einer Standardposition im Clientsystem gespeichert werden.

Syntax



Parameter

Knotenname

Der den Protokolldateien zugeordnete Clientknotenname. Bei den meisten Clientsystemen wird nur ein Knotenname auf dem IBM Spectrum Protect-Server registriert. Auf Systemen mit mehreren Benutzern, z. B. Linux-Clientsysteme, kann es jedoch mehrere Clientknotennamen geben. Dieser Parameter ist erforderlich.

Server-IP

Die TCP/IP-Adresse des IBM Spectrum Protect-Servers, auf dem der Clientverwaltungsservice authentifiziert wird. Dieser Parameter ist erforderlich.

Sie können eine aus 1 - 64 Zeichen bestehende TCP/IP-Adresse für den Server angeben. Die Serveradresse kann ein TCP/IP-Domänenname oder eine numerische IP-Adresse sein. Die numerische IP-Adresse kann eine TCP/IP-Adresse der Version 4 oder der Version 6 sein. Sie können IPv6-Adressen nur verwenden, wenn die Option **`commmethod V6Tcpip`** für das Clientsystem angegeben ist.

Beispiele:

- `server.example.com`
- `192.0.2.0`
- `2001:0DB8:0:0:0:0:0:0`

Server-Port

Die TCP/IP-Anschlussnummer, die für die Kommunikation mit dem IBM Spectrum Protect-Server verwendet wird. Sie können einen Wert im Bereich von 1 bis 32767 angeben. Dieser Parameter ist erforderlich.

Beispiel: `1500`

Serverprotokoll

Das für die Kommunikation zwischen dem Clientverwaltungsservice und dem IBM Spectrum Protect-Server verwendete Protokoll. Dieser Parameter ist erforderlich.

Sie können einen der folgenden Werte angeben.

Wert	Bedeutung
NO_SSL	Das SSL-Sicherheitsprotokoll wird nicht verwendet.
SSL	Das SSL-Sicherheitsprotokoll wird verwendet.
FIPS	Das Protokoll TLS 1.2 wird im FIPS-Modus (Federal Information Processing Standard) verwendet. **Tipp:** Sie können auch `TLS_1.2` eingeben, um anzugeben, dass das Protokoll TLS 1.2 im FIPS-Modus verwendet wird.

OptPfad
Der vollständig qualifizierte Pfad der Clientoptionsdatei. Dieser Parameter ist erforderlich.

Beispiel für Linux-Client: `/opt/backup_tools/tivoli/tsm/baclient/dsm.sys`

Beispiel für Windows-Client: `C:\backup tools\Tivoli\TSM\baclient\dsm.opt`

Beispiel für ein Linux-Clientsystem

Die Knotendefinition für den Clientknoten SUSAN zur Datei `client-configuration.xml` hinzufügen. Der Knoten kommuniziert mit dem IBM Spectrum Protect-Server `server.example.com` an Serveranschluss `1500`. Das SSL-Sicherheitsprotokoll wird nicht verwendet. Der Pfad für die Clientsystemoptionsdatei lautet `/opt/tivoli/tsm/client/ba/bin/custom_opt.sys`.

Geben Sie den folgenden Befehl im Verzeichnis `/opt/tivoli/tsm/cms/bin` aus.

Befehl:
```
./CmsConfig.sh addnode SUSAN server.example.com 1500 NO_SSL /opt/tivoli/tsm/client/ba/bin/custom_opt.sys
```

Ausgabe:

```
Knoten wird hinzugefügt.

Hinzufügen der Clientkonfiguration beendet.
```

Beispiel für ein Windows-Clientsystem

Die Knotendefinition für den Clientknoten SUSAN zur Datei `client-configuration.xml` hinzufügen. Der Knoten kommuniziert mit dem IBM Spectrum Protect-Server `server.example.com` an Serveranschluss `1500`. Das SSL-Sicherheitsprotokoll wird nicht verwendet. Der Pfad für die Clientoptionsdatei lautet `c:\program files\tivoli\tsm\baclient\custom.opt`.

Geben Sie den folgenden Befehl im Verzeichnis `C:\Programme\Tivoli\TSM\cms\bin` aus.

Befehl:
```
cmsconfig addnode SUSAN server.example.com 1500 NO_SSL "c:\program files\tivoli\tsm\baclient\custom.opt"
```

Ausgabe:

```
Knoten wird hinzugefügt.

Hinzufügen der Clientkonfiguration beendet.
```

Befehl `CmsConfig setopt`

Mit dem Befehl **`CmsConfig setopt`** können Sie den Pfad der Clientoptionsdatei (normalerweise `dsm.opt`) für eine vorhandene Knotendefinition festlegen, ohne den Inhalt der Clientoptionsdatei vorher zu lesen.

Dieser Befehl ist hilfreich, wenn die Clientoptionsdatei keinen Standardnamen hat oder sich nicht an der Standardposition befindet.

Voraussetzungen: Ist die Knotendefinition nicht vorhanden, müssen Sie zunächst den Befehl **CmsConfig addnode** ausgeben, um sie zu erstellen.

Anders als der Befehl **CmsConfig discover** erstellt der Befehl **CmsConfig setopt** keine zugehörigen Protokolldefinitionen in der Datei `client-configuration.xml`. Sie müssen die Protokolldefinitionen mit dem Befehl **CmsComfog addlog** erstellen.

Syntax

Parameter

Knotenname
Der den Protokolldateien zugeordnete Clientknotenname. Bei den meisten Clientsystemen wird nur ein Knotenname auf dem IBM Spectrum Protect-Server registriert. Auf Systemen mit mehreren Benutzern, z. B. Linux-Clientsysteme, kann es jedoch mehrere Clientknotennamen geben. Dieser Parameter ist erforderlich.

OptPfad
Der vollständig qualifizierte Pfad der Clientoptionsdatei. Dieser Parameter ist erforderlich.

Beispiel für Linux-Client: `/opt/backup_tools/tivoli/tsm/baclient/dsm.opt`

Beispiel für Windows-Client: `C:\backup tools\Tivoli\TSM\baclient\dsm.opt`

Beispiel für ein Linux-Clientsystem

Den Pfad der Clientoptionsdatei für den Knoten SUSAN definieren. Der Pfad für die Clientoptionsdatei lautet `/opt/tivoli/tsm/client/ba/bin/dsm.opt`.

Geben Sie den folgenden Befehl im Verzeichnis `/opt/tivoli/tsm/cms/bin` aus.

Befehl:

```
./CmsConfig.sh setopt SUSAN /opt/tivoli/tsm/client/ba/bin/dsm.opt
```

Ausgabe:

```
Knotenkonfigurationsdatei wird hinzugefügt.

Hinzufügen der Clientkonfigurationsdatei beendet.
```

Beispiel für ein Windows-Clientsystem

Den Pfad der Clientoptionsdatei für den Knoten SUSAN definieren. Der Pfad für die Clientoptionsdatei lautet `c:\Programme\tivoli\tsm\baclient\dsm.opt`.

Geben Sie den folgenden Befehl im Verzeichnis `C:\Programme\Tivoli\TSM\cms\bin` aus.

Befehl:

```
cmsconfig setopt SUSAN "c:\program files\tivoli\tsm\baclient\dsm.opt"
```

Ausgabe:

```
Knotenkonfigurationsdatei wird hinzugefügt.

Hinzufügen der Clientkonfigurationsdatei beendet.
```

Befehl CmsConfig setsys

Auf einem Linux-Clientsystem können Sie mit dem Befehl **CmsConfig setsys** den Pfad der Clientsystemoptionsdatei (normalerweise `dsm.sys`) für eine vorhandene Knotendefinition festlegen, ohne den Inhalt der Clientsystemoptionsdatei vorher zu lesen.

Dieser Befehl ist hilfreich, wenn die Clientsystemoptionsdatei keinen Standardnamen hat oder sich nicht an der Standardposition befindet.

Voraussetzungen: Ist die Knotendefinition nicht vorhanden, müssen Sie zunächst den Befehl **CmsConfig addnode** ausgeben, um sie zu erstellen.

Anders als der Befehl **CmsConfig discover** erstellt der Befehl **CmsConfig setsys** keine zugehörigen Protokolldefinitionen in der Datei `client-configuration.xml`. Sie müssen die Protokolldefinitionen mit dem Befehl **CmsComfog addlog** erstellen.

Syntax

Parameter

Knotenname
Der den Protokolldateien zugeordnete Clientknotenname. Bei den meisten Clientsystemen wird nur ein Knotenname auf dem IBM Spectrum Protect-Server registriert. Auf Systemen mit mehreren Benutzern, z. B. Linux-Clientsysteme, kann es jedoch mehrere Clientknotennamen geben. Dieser Parameter ist erforderlich.

SysPfad
Der vollständig qualifizierte Pfad der Clientsystemoptionsdatei. Dieser Parameter ist erforderlich.

Beispiel: `/opt/backup_tools/tivoli/tsm/baclient/dsm.sys`

Beispiel

Den Pfad der Clientsystemoptionsdatei für den Knoten SUSAN definieren. Der Pfad für die Clientsystemoptionsdatei lautet `/opt/tivoli/tsm/client/ba/bin/dsm.sys`.

Geben Sie den folgenden Befehl im Verzeichnis `/opt/tivoli/tsm/cms/bin` aus.

Befehl:

```
./CmsConfig.sh setopt SUSAN /opt/tivoli/tsm/client/ba/bin/dsm.sys
```

Ausgabe:

```
Knotenkonfigurationsdatei wird hinzugefügt.

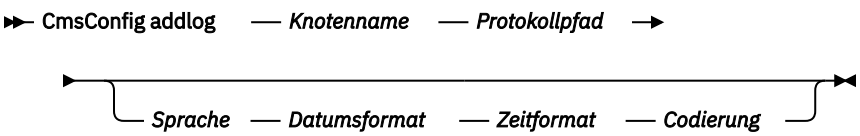
Hinzufügen der Clientkonfigurationsdatei beendet.
```

Befehl CmsConfig addlog

Mit dem Befehl **CmsConfig addlog** können Sie die Position von Clientprotokolldateien einer vorhandenen Knotendefinition in der Konfigurationsdatei `client-configuration.xml` manuell hinzufügen. Verwenden Sie diesen Befehl nur, wenn die Clientprotokolldateien nicht an einer Standardposition im Clientsystem gespeichert werden.

Voraussetzungen: Ist die Knotendefinition nicht vorhanden, müssen Sie zunächst den Befehl **CmsConfig addnode** ausgeben, um sie zu erstellen.

Syntax



Parameter

Knotenname
Der den Protokolldateien zugeordnete Clientknotenname. Bei den meisten Clientsystemen wird nur ein Knotenname auf dem IBM Spectrum Protect-Server registriert. Auf Systemen mit mehreren Benutzern, z. B. Linux-Clientsysteme, kann es jedoch mehrere Clientknotennamen geben. Dieser Parameter ist erforderlich.

Protokollpfad
Der vollständig qualifizierte Pfad der Protokolldateien. Dieser Parameter ist erforderlich.

Beispiel für Linux-Client: `/opt/backup_tools/tivoli/tsm/baclient/dsmerror.log`

Beispiel für Windows-Client: `C:\backup tools\Tivoli\TSM\baclient\dsmerror.log`

Sprache
Die Spracheinstellung der Protokolldatei. Dieser Parameter ist optional. Wenn Sie diesen Parameter angeben, müssen Sie jedoch auch die Parameter **`Datumsformat`**, **`Zeitformat`** und **`Codierung`** angeben. Sie müssen die Ländereinstellung für folgende Sprachen angeben.

Sprache	**Ländereinstellung**
Portugiesisch, Brasilianisches	`pt_BR`
Chinesisch, vereinfacht	`zh_CN`
Chinesisch, traditionell	`zh_TW`
Tschechisch	`cs_CZ`
Englisch	`en_US`
Französisch	`fr_FR`
Deutsch	`de_DE`
Ungarisch	`hu_HU`
Italienisch	`it_IT`
Japanisch	`ja_JP`
Koreanisch	`ko_KR`
Polnisch	`pl_PL`
Russisch	`ru_RU`
Spanisch	`es_ES`

Datumsformat
Das Datumsformat der Zeitmarkeneinträge in der Clientprotokolldatei. Dieser Parameter ist optional. Wenn Sie diesen Parameter angeben, müssen Sie jedoch auch die Parameter **`Sprache`**, **`Zeitformat`** und **`Codierung`** angeben.

Die folgende Tabelle enthält die Datumsformate für die Sprachen.

Tipp: Anstelle der in der Tabelle aufgelisteten Datumsformate können Sie ein Datumsformat mit der Option **`dateformat`** des Clients für Sichern/Archivieren angeben.

Sprache	**Datumsformat**
Chinesisch, vereinfacht	`yyyy-MM-dd`
Chinesisch, traditionell	`yyyy/MM/dd`
Tschechisch	`dd.MM.yyyy`

Sprache	Datumsformat
Englisch	MM/dd/yyyy
Französisch	dd/MM/yyyy
Deutsch	dd.MM.yyyy
Ungarisch	yyyy.MM.dd
Italienisch	dd/MM/yyyy
Japanisch	yyyy-MM-dd
Koreanisch	yyyy/MM/dd
Polnisch	yyyy-MM-dd
Portugiesisch, Brasilianisches	dd/MM/yyyy
Russisch	dd.MM.yyyy
Spanisch	dd.MM.yyyy

Zeitformat

Das Zeitformat der Zeitmarkeneinträge in der Clientprotokolldatei. Dieser Parameter ist optional. Wenn Sie diesen Parameter angeben, müssen Sie jedoch auch die Parameter **Sprache**, **Datumsformat** und **Codierung** angeben.

Die folgende Tabelle enthält Beispiele für Standardzeitformate, die Sie für Clientbetriebssysteme angeben können.

Tipp: Anstelle der in der Tabelle aufgelisteten Zeitformate können Sie ein Zeitformat mit der Option **timeformat** des Clients für Sichern/Archivieren angeben.

Sprache	Zeitformat für Linux-Clientsysteme	Zeitformat für Windows-Clientsysteme
Chinesisch, vereinfacht	HH:mm:ss	HH:mm:ss
Chinesisch, traditionell	HH:mm:ss	ahh:mm:ss
Tschechisch	HH:mm:ss	HH:mm:ss
Englisch	HH:mm:ss	HH:mm:ss
Französisch	HH:mm:ss	HH:mm:ss
Deutsch	HH:mm:ss	HH:mm:ss
Ungarisch	HH.mm.ss	HH:mm:ss
Italienisch	HH:mm:ss	HH:mm:ss
Japanisch	HH:mm:ss	HH:mm:ss
Koreanisch	HH:mm:ss	HH:mm:ss
Polnisch	HH:mm:ss	HH:mm:ss
Portugiesisch, Brasilianisches	HH:mm:ss	HH:mm:ss
Russisch	HH:mm:ss	HH:mm:ss
Spanisch	HH:mm:ss	HH:mm:ss

Codierung
Die Zeichencodierung der Einträge in den Clientprotokolldateien. Dieser Parameter ist optional. Wenn Sie diesen Parameter angeben, müssen Sie jedoch auch die Parameter **Sprache**, **Datumsformat** und **Zeitformat** angeben.

Für Linux-Clientsysteme ist die Standardzeichencodierung UTF-8. Für Windows-Clientsysteme sind die Standardcodierungswerte in der folgenden Tabelle aufgeführt. Ist Ihr Clientsystem anders angepasst, verwenden Sie den Parameter **Codierung**, um einen vom Standardwert abweichenden Wert anzugeben.

Sprache	Codierung
Chinesisch, vereinfacht	CP936
Chinesisch, traditionell	CP950
Tschechisch	Windows-1250
Englisch	Windows-1252
Französisch	Windows-1252
Deutsch	Windows-1252
Ungarisch	Windows-1250
Italienisch	Windows-1252
Japanisch	CP932
Koreanisch	CP949
Polnisch	Windows-1250
Portugiesisch, Brasilianisches	Windows-1252
Russisch	Windows-1251
Spanisch	Windows-1252

Beispiel für ein Linux-Clientsystem

Die Position der Clientprotokolldatei der vorhandenen Definition für Clientknoten SUSAN in der Datei `client-configuration.xml` hinzufügen. Der Pfad für die Clientprotokolldatei lautet `/usr/work/logs/dsmerror.log`. Die Sprachenspezifikation, das Zeitformat und das Datumsformat für die Ländereinstellung 'Französisch' hinzufügen.

Geben Sie den folgenden Befehl im Verzeichnis `/opt/tivoli/tsm/cms/bin` aus.

Befehl:

```
./CmsConfig.sh addlog SUSAN /usr/work/logs/dsmerror.log fr_FR yyyy/MM/dd
HH:MM:ss UTF-8
```

Ausgabe:

```
Protokoll wird hinzugefügt.

Hinzufügen des Protokolls beendet.
```

Beispiel für ein Windows-Clientsystem

Die Position der Clientprotokolldatei der vorhandenen Definition für Clientknoten SUSAN in der Datei `client-configuration.xml` hinzufügen. Der Pfad für die Clientprotokolldatei lautet `c:\work\logs\dsmerror.log`. Die Sprachenspezifikation, das Zeitformat und das Datumsformat für die Ländereinstellung 'Französisch' hinzufügen.

Geben Sie den folgenden Befehl im Verzeichnis `C:\Programme\Tivoli\TSM\cms\bin` aus.

Befehl:

```
cmsconfig addlog SUSAN c:\work\logs\dsmerror.log fr_FR yyyy/MM/dd HH:MM:ss
UTF-8
```

Ausgabe:

```
Protokoll wird hinzugefügt.

Hinzufügen des Protokolls beendet.
```

Befehl CmsConfig remove

Mit dem Befehl **CmsConfig remove** können Sie eine Clientknotendefinition aus der Clientkonfigurationsdatei `client-configuration.xml` entfernen. Alle dem Clientknotennamen zugeordneten Protokolldateieinträge werden ebenfalls entfernt.

Syntax

Parameter

Knotenname
Der den Protokolldateien zugeordnete Clientknotenname. Bei den meisten Clientsystemen wird nur ein Knotenname auf dem IBM Spectrum Protect-Server registriert. Auf Systemen mit mehreren Benutzern, z. B. Linux-Clientsysteme, kann es jedoch mehrere Clientknotennamen geben. Dieser Parameter ist erforderlich.

Beispiel für ein Linux-Clientsystem

Die Knotendefinition für SUSAN aus der Datei `client-configuration.xml` entfernen.

Geben Sie den folgenden Befehl im Verzeichnis `/opt/tivoli/tsm/cms/bin` aus.

Befehl:

```
./CmsConfig.sh remove SUSAN
```

Ausgabe:

```
Knoten wird entfernt.

Entfernen des Knotens beendet.
```

Beispiel für ein Windows-Clientsystem

Die Knotendefinition für SUSAN aus der Datei `client-configuration.xml` entfernen.

Geben Sie den folgenden Befehl im Verzeichnis `C:\Programme\Tivoli\TSM\cms\bin` aus.

Befehl:

```
cmsconfig remove SUSAN
```

Ausgabe:

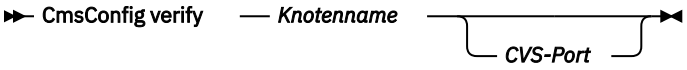
```
Knoten wird entfernt.

Entfernen des Knotens beendet.
```

Befehl CmsConfig verify

Mit dem Befehl **CmsConfig verify** können Sie überprüfen, ob eine Knotendefinition in der Datei `client-configuration.xml` ordnungsgemäß erstellt wurde. Liegen Knotendefinitionsfehler vor oder ist der Knoten nicht ordnungsgemäß definiert, müssen Sie die Knotendefinition mit den entsprechenden **CmsConfig**-Befehlen korrigieren.

Syntax



Parameter

Knotenname
Der den Protokolldateien zugeordnete Clientknotenname. Bei den meisten Clientsystemen wird nur ein Knotenname auf dem IBM Spectrum Protect-Server registriert. Auf Systemen mit mehreren Benutzern, z. B. Linux-Clientsysteme, kann es jedoch mehrere Clientknotennamen geben. Dieser Parameter ist erforderlich.

CVS-Port
Die TCP/IP-Anschlussnummer, die für die Kommunikation mit dem Clientverwaltungsservice verwendet wird. Geben Sie die Anschlussnummer an, wenn Sie während der Installation des Clientverwaltungsservice nicht die Standardanschlussnummer verwendet haben. Die Standardanschlussnummer ist 9028. Dieser Parameter ist optional.

Beispiel für ein Linux-Clientsystem

Sicherstellen, dass die Knotendefinition für den Knoten SUSAN in der Datei `client-configuration.xml` ordnungsgemäß erstellt wird.

Geben Sie den folgenden Befehl im Verzeichnis `/opt/tivoli/tsm/cms/bin` aus.

Befehl:

```
./CmsConfig.sh verify SUSAN
```

Während des Prüfprozesses werden Sie zur Eingabe des Clientknotennamens oder der ID und des Kennworts für den Benutzer mit Verwaltungsaufgaben aufgefordert.

Ausgabe:

```
Knoten wird überprüft.


Die CMS-Servicekonfiguration für Knoten SUSAN wird überprüft.
Die CMS-Konfiguration sieht korrekt aus.

Ordnungsgemäße Funktionsweise des CMS-Service an Anschluss 9028 wird überprüft.

Benutzer-ID eingeben: admin
Kennwort eingeben:

Verbindung zum CMS-Service wird hergestellt und Ressourcen werden überprüft.
Der CMS-Service arbeitet ordnungsgemäß.
Knotenüberprüfung beendet.
```

Beispiel für ein Windows-Clientsystem

Sicherstellen, dass die Knotendefinition für den Knoten SUSAN in der Datei `client-configuration.xml` ordnungsgemäß erstellt wird.

Geben Sie den folgenden Befehl im Verzeichnis `C:\Programme\Tivoli\TSM\cms\bin` aus.

Befehle:

```
cmsconfig verify SUSAN
```

Während des Prüfprozesses werden Sie zur Eingabe des Clientknotennamens oder der ID und des Kennworts für den Benutzer mit Verwaltungsaufgaben aufgefordert.

Ausgabe:

```
Knoten wird überprüft.
```

```
Die CMS-Servicekonfiguration für Knoten SUSAN wird überprüft.
Die CMS-Konfiguration sieht korrekt aus.

Ordnungsgemäße Funktionsweise des CMS-Service an Anschluss 9028 wird überprüft.

Benutzer-ID eingeben: admin
Kennwort eingeben:

Verbindung zum CMS-Service wird hergestellt und Ressourcen werden überprüft.
Der CMS-Service arbeitet ordnungsgemäß.
Knotenüberprüfung beendet.
```

Befehl CmsConfig list

Mit dem Befehl **CmsConfig list** können Sie die Konfiguration des Clientverwaltungsservice anzeigen.

Syntax

Beispiel für ein Linux-Clientsystem

Konfiguration des Clientverwaltungsservice anzeigen. Anschließend die Ausgabe überprüfen, um sicherzustellen, dass der Befehl richtig eingegeben wurde.

Geben Sie den folgenden Befehl im Verzeichnis `/opt/tivoli/tsm/cms/bin` aus.

Befehl:

```
./CmsConfig.sh list
```

Ausgabe:

```
CMS-Konfiguration auflisten

server.example.com:1500 NO_SSL SUSAN
          Funktionen: [LOG_QUERY]
    Optionsdateipfad: /opt/tivoli/tsm/client/ba/bin/dsm.sys

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

Beispiel für ein Windows-Clientsystem

Konfiguration des Clientverwaltungsservice anzeigen. Anschließend die Ausgabe überprüfen, um sicherzustellen, dass der Befehl richtig eingegeben wurde.

Geben Sie den folgenden Befehl im Verzeichnis `C:\Programme\Tivoli\TSM\cms\bin` aus.

Befehl:

```
cmsconfig list
```

Ausgabe:

```
CMS-Konfiguration auflisten

server.example.com:1500 NO_SSL SUSAN
          Funktionen: [LOG_QUERY]
    Optionsdateipfad: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

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

Befehl `CmsConfig help`

Mit dem Befehl **`CmsConfig help`** können Sie die Syntax der Befehle des Dienstprogramms **`CmsConfig`** anzeigen.

Syntax

Beispiel für ein Linux-Clientsystem

Geben Sie den folgenden Befehl im Verzeichnis `/opt/tivoli/tsm/cms/bin` aus:

```
./CmsConfig help
```

Beispiel für ein Windows-Clientsystem

Geben Sie den folgenden Befehl im Verzeichnis `C:\Programme\Tivoli\TSM\cms\bin` aus:

```
CmsConfig help
```

Erweiterte Funktionalität des Clientverwaltungsservice

Der IBM Spectrum Protect-Clientverwaltungsservice erfasst Daten standardmäßig nur aus Clientprotokolldateien. Um andere Clientaktionen einzuleiten, können Sie auf die im Clientverwaltungsservice enthaltene REST-API zugreifen (REST = Representational State Transfer).

API-Entwickler können REST-Anwendungen erstellen, um die folgenden Clientaktionen einzuleiten:

- Clientoptionsdateien abfragen und aktualisieren (z. B. Datei `dsm.sys` auf Linux-Clients und Datei `dsm.opt` auf Linux- und Windows-Clients)
- Status des IBM Spectrum Protect-Clientakzeptordämons und des Schedulers abfragen
- Dateien für einen Clientknoten sichern und zurückschreiben
- Funktionalität des Clientverwaltungsservice mit Scripts erweitern

Ausführliche Informationen zur REST-API des Clientverwaltungsservice finden Sie in Client Management Services REST API Guide.

Kapitel 12. Fehlerbehebung für die Operations Center-Installation

Wenn bei der Installation des Operations Center ein Problem auftritt, das Sie nicht lösen können, können Sie in den Beschreibungen der bekannten Probleme nach einer Lösungsmöglichkeit suchen.

Chinesische, japanische oder koreanische Schriftarten werden nicht ordnungsgemäß angezeigt

Chinesische, japanische oder koreanische Schriftarten werden im Operations Center unter Red Hat Enterprise Linux 5 nicht ordnungsgemäß angezeigt.

Lösung

Installieren Sie die folgenden Schriftartpakete, die von Red Hat verfügbar sind:

- fonts-chinese
- fonts-japanese
- fonts-korean

Kapitel 13. Operations Center deinstallieren

Sie können das Operations Center mit jeder der folgenden Methoden deinstallieren: grafischer Assistent, Befehlszeile im Konsolenmodus oder unbeaufsichtigter Modus.

Operations Center mit einem grafisch orientierten Assistenten deinstallieren

Sie können das Operations Center mithilfe des grafisch orientierten Assistenten von IBM Installation Manager deinstallieren.

Vorgehensweise

1. Öffnen Sie IBM Installation Manager.

   In dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das Unterverzeichnis `eclipse` (z. B. `/opt/IBM/InstallationManager/eclipse`) und geben Sie folgenden Befehl aus:

   ```
   ./IBMIM
   ```

2. Klicken Sie auf **Deinstallieren**.
3. Wählen Sie die Option für das Operations Center aus und klicken Sie auf **Weiter**.
4. Klicken Sie auf **Deinstallieren**.
5. Klicken Sie auf **Fertigstellen**.

Operations Center im Konsolenmodus deinstallieren

Zum Deinstallieren des Operations Center mithilfe der Befehlszeile müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit dem Parameter für den Konsolenmodus ausführen.

Vorgehensweise

1. In dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:

   `eclipse/tools`

   Beispiel:

   `/opt/IBM/InstallationManager/eclipse/tools`
2. Im Verzeichnis `tools` geben Sie den folgenden Befehl aus:

   `./imcl -c`
3. Für die Deinstallation geben Sie 5 ein.
4. Wählen Sie die Deinstallation aus der IBM Spectrum Protect-Paketgruppe aus.
5. Geben Sie N für 'Next' (Weiter) ein.
6. Wählen Sie die Deinstallation des Operations Center-Pakets aus.
7. Geben Sie N für 'Next' (Weiter) ein.
8. Geben Sie U für 'Uninstall' (Deinstallieren) ein.
9. Geben Sie F für 'Finish' (Fertigstellen) ein.

Operations Center im unbeaufsichtigten Modus deinstallieren

Zum Deinstallieren des Operations Center im unbeaufsichtigten Modus müssen Sie das Deinstallationsprogramm von IBM Installation Manager über die Befehlszeile mit den Parametern für den unbeaufsichtigten Modus ausführen.

Vorbereitende Schritte

Sie können die Dateneingabe für eine unbeaufsichtigte Deinstallation des Operations Center-Servers mithilfe einer Antwortdatei bereitstellen. IBM Spectrum Protect enthält eine Musterantwortdatei, `uninstall_response_sample.xml`, im Verzeichnis `input`, in dem das Installationspaket extrahiert wird. Diese Datei enthält Standardwerte, durch die Sie unnötige Warnungen vermeiden können.

Wenn Sie das Operations Center deinstallieren wollen, lassen Sie die Einstellung `modify="false"` für den Operations Center-Eintrag in der Antwortdatei unverändert.

Wenn Sie die Antwortdatei anpassen wollen, können Sie die in der Datei enthaltenen Optionen ändern. Informationen zu Antwortdateien finden Sie in Antwortdateien.

Vorgehensweise

1. In dem Verzeichnis, in dem IBM Installation Manager installiert ist, wechseln Sie in das folgende Unterverzeichnis:

   ```
   eclipse/tools
   ```

   Beispiel:

   ```
   /opt/IBM/InstallationManager/eclipse/tools
   ```

2. Im Verzeichnis `tools` geben Sie den folgenden Befehl aus, wobei *Antwortdatei* den Pfad der Antwortdatei einschließlich des Dateinamens angibt:

   ```
   ./imcl -input Antwortdatei -silent
   ```

   Der folgende Befehl ist ein Beispiel:

   ```
   ./imcl -input /tmp/input/uninstall_response.xml -silent
   ```

Kapitel 14. Rollback zu einer vorherigen Version des Operations Center durchführen

Standardmäßig speichert IBM Installation Manager ältere Versionen eines Pakets, damit ein Rollback ausgeführt werden kann, falls Probleme mit neueren Versionen von Updates, Fixes oder Paketen auftreten.

Vorbereitende Schritte

Die Rollback-Funktion ist erst verfügbar, nachdem das Operations Center aktualisiert wurde.

Informationen zu diesem Vorgang

Wenn IBM Installation Manager ein Rollback zu einer vorherigen Version durchführt, wird die aktuelle Version der Paketdateien deinstalliert und die frühere Version erneut installiert.

Um ein Rollback zu einer vorherigen Version durchführen zu können, muss IBM Installation Manager auf Dateien für diese Version zugreifen. Diese Dateien werden standardmäßig während jeder aufeinanderfolgenden Installation gespeichert. Da die Anzahl der gespeicherten Dateien bei jeder installierten Version zunimmt, sollten Sie diese Dateien regelmäßig aus Ihrem System löschen. Wenn Sie die Dateien löschen, können Sie jedoch kein Rollback zu einer vorherigen Version durchführen.

Gehen Sie wie folgt vor, um gespeicherte Dateien zu löschen oder um Ihre Einstellung für die Speicherung dieser Dateien bei zukünftigen Installationen zu aktualisieren:

1. Klicken Sie in IBM Installation Manager auf **Datei** > **Benutzervorgaben**.
2. Klicken Sie auf der Seite mit den **Benutzervorgaben** auf **Dateien für Rollback** und geben Sie Ihre Vorgaben an.

Prozedur

- Wenn Sie ein Rollback zu einer vorherigen Version des Operations Center ausführen möchten, verwenden Sie die Funktion **Rollback durchführen** von IBM Installation Manager.

Anhang A. Installationsprotokolldateien

Wenn während der Installation Fehler auftreten, werden diese in Protokolldateien aufgezeichnet, die im IBM Installation Manager-Verzeichnis 'logs' gespeichert werden.

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

Anhang B. 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 International Business Machines Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Herstellern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "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 der zugehörigen Tochtergesellschaften in den USA und/oder anderen Ländern.

Die eingetragene Marke Linux wird gemäß einer Unterlizenz der Linux Foundation verwendet, dem exklusiven Lizenznehmer von Linus Torvalds, dem Eigentümer der Marke auf einer weltweiten Basis.

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.

Red Hat, OpenShift®, Ansible® und Ceph® sind Marken oder eingetragene Marken der Red Hat, Inc. oder der zugehörigen Tochtergesellschaften in den USA und/oder anderen Ländern.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

VMware, VMware vCenter Server und VMware vSphere sind eingetragene Marken oder Marken der VMware, Inc. oder ihrer Tochtergesellschaften in den USA oder 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 weder weitergeben oder anzeigen noch 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 weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Berechtigungen
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 Vorschriften, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

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 bereitgestellten 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 rechtlich beraten lassen, insbesondere Meldepflichten sowie die Einforderung von Einwilligungen.

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

Für die IBM Spectrum Protect-Produktfamilie steht ein Glossar mit Begriffen und Definitionen zur Verfügung.

Siehe das Glossar für IBM Spectrum Protect.

Index

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z

Programmnummer: 5725-W99
5725-W98
5725-X15