IBM Spectrum Protect Plus
Version 10.1.4

Installations- und Benutzerhandbuch

Hinweis:

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen” auf Seite 335 gelesen werden.

Diese Ausgabe bezieht sich auf Version 10, Release 1, Modifikation 4 von IBM Spectrum Protect Plus (Produktnummer 5737-F11) und auf alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

© Copyright International Business Machines Corporation 2017, 2019.

Inhaltsverzeichnis

Zu dieser Veröffentlichung

Diese Veröffentlichung enthält eine Übersicht, sowie Planungs-, Installations- und Benutzeranweisungen für IBM Spectrum Protect Plus.

Zielgruppe dieser Veröffentlichung

Diese Veröffentlichung richtet sich an Administratoren und Benutzer, die für die Implementierung einer Sicherungs- und Wiederherstellungslösung mit IBM Spectrum Protect Plus in einer der unterstützten Umgebungen verantwortlich sind.

In dieser Veröffentlichung wird vorausgesetzt, dass Sie über Kenntnisse in den Anwendungen verfügen, die von IBM Spectrum Protect Plus unterstützt werden (siehe „Systemanforderungen” auf Seite 11).

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®.

Zum Anzeigen der IBM Produktdokumentation siehe IBM Knowledge Center.

© Copyright IBM Corp. 2017, 2019

Neuerungen in Version 10.1.4

In IBM Spectrum Protect Plus Version 10.1.4 werden neue Funktionen und Aktualisierungen eingeführt.

Eine Liste der neuen Funktionen und Aktualisierungen in diesem Release und vorheriger Releases von Version 10 finden Sie in Aktualisierungen für IBM Spectrum Protect Plus.

Neue und geänderte Informationen in dieser Produktdokumentation sind links neben der Änderung durch einen vertikalen Strich (|) angegeben.

© Copyright IBM Corp. 2017, 2019

Bei der Produktentwicklung mitwirken

Sie können Einfluss auf die Zukunft von IBM Speicherprodukten nehmen, indem Sie Ihre Kenntnisse mit den Designer- und Entwicklerteams teilen. Um mitzuwirken, beteiligen Sie sich am Sponsorbenutzerprogramm oder am Betaprogramm.

Sponsorbenutzerprogramm

Das IBM Storage-Sponsorbenutzerprogramm ermöglicht es Ihnen, direkt mit Designern und Entwicklern zu arbeiten, um Einfluss auf die Ausrichtung der Produkte zu nehmen, die Sie verwenden.

IBM lädt Sie ein, Ihre Erfahrung und Ihr Fachwissen mit anderen zu teilen. Wenn Sie sich an dem Programm beteiligen, helfen Sie uns bei der Erkundung und der potenziellen Implementierung neuer Produktfunktionen, die für Sie und Ihr Unternehmen wichtig sind.

Verwenden Sie ein IBM Speichersoftwareprodukt wie z. B. IBM Spectrum Protect Plus?

Sind Sie bereit, Ihre Vision zu teilen?

Dann melden Sie sich für das Sponsorbenutzerprogramm an, um an dem Produktinnovationsprozess mitzuwirken. Außerdem können Sie als Sponsorbenutzer bevorstehende Speicherreleases voranzeigen und bei Betaprogrammen mitwirken, um neue Produktfunktionen zu testen.

Um sich an dem Sponsorbenutzerprogramm zu beteiligen oder zusätzliche Informationen anzufordern, füllen Sie das folgende Formular aus:

IBM Storage Sponsor User

Ihre Informationen werden vertraulich behandelt und werden von den IBM Designer- und Entwicklerteams nur zu Produktentwicklungszwecken verwendet.

Betaprogramm

Das IBM Spectrum Protect Plus-Betaprogramm gibt Ihnen einen ersten Einblick in bevorstehende Produktfunktionen und eine Möglichkeit, Einfluss auf Entwurfsänderungen zu nehmen. Sie können neue Software in Ihrer Umgebung testen und haben direkten Einfluss auf den Produktentwicklungsprozess.

Das Betaprogramm ist für eine Vielzahl von Beteiligten attraktiv, einschließlich Kunden, IBM Business Partner und IBM Mitarbeiter.

Das Programm bietet die folgenden Vorteile:

Zugriff auf Code in einem frühen Stadium und Auswertung neuer Produktfunktionen und Erweiterungen
Sie erhalten Zugriff auf den Betacode vor der allgemeinen Verfügbarkeit des Produktrelease, um zu bestimmen, ob die neuen Funktionen und Erweiterungen gut zu Ihrer Organisation passen. Nach dem Herunterladen des Codes können Sie die neue Software in Ihrer Umgebung ausführen und validieren. Sie können dann alle Probleme identifizieren und beheben, bevor der Code verfügbar ist. Damit sparen Sie Zeit und helfen Sie, spätere Probleme in der Produktion zu verhindern. Wenn der Code verfügbar wird, sind Sie für die Installation bereit und können Sie die Vorteile der neuen Funktionen nutzen.

Interaktion mit Designer- und Entwicklerteams
Die Produktdesigner, Architekten, Entwickler und Tester helfen bei der Planung der Betaversion und unterstützen die Beteiligten. Diese Experten können Sie bei der Behebung von Problemen unterstützen.

Ein IBM Referenzkunde werden
Nach Ihrer positiven Erfahrung mit dem Betaprogramm werden Sie von IBM eingeladen, am Referenzprogramm teilzunehmen. Das IBM Marketing-Team hilft Ihnen bei der Erstellung einer Nachricht, mit

© Copyright IBM Corp. 2017, 2019

der Sie anderen potenziellen Betatestern Ihren Erfolg bei der Übernahme und Verwendung des frühzeitigen Codes mitteilen können.

Kontaktinformationen und Angaben zur Registrierung

Für weitere Informationen zum Betaprogramm wenden Sie sich an Mary Anne Filosa unter mailto:mfilosa@us.ibm.com.

Sie können sich registrieren, indem Sie das Anmeldeformular für das IBM Spectrum Protect Plus-Betaprogramm ausfüllen.

Kapitel 1. IBM Spectrum Protect Plus - Übersicht

IBM Spectrum Protect Plus ist eine Lösung für den Datenschutz und zur Gewährleistung der Verfügbarkeit in virtuellen Umgebungen und für Datenbankanwendungen, die innerhalb von Minuten implementiert werden und Ihre Umgebung innerhalb einer Stunde schützen kann.

IBM Spectrum Protect Plus kann als Standalone-Lösung implementiert werden oder in Cloudspeicher oder in einen Repository-Server (z. B. ein IBM Spectrum Protect-Server) integriert werden, um Kopien zur langfristigen Speicherung auszulagern.

Produktkomponenten

Die IBM Spectrum Protect Plus-Lösung wird als unabhängige virtuelle Appliance bereitgestellt, die Speicher- und Datenversetzungskomponenten enthält.

Anforderungen für die Festlegung der Komponentenzahl: In einigen Umgebungen sind unter Umständen mehr Instanzen dieser Komponenten erforderlich, um größere Arbeitslasten unterstützen zu können. Anweisungen zur Festlegung der Anzahl Komponenten sowie zur Erstellung und Integration von Komponenten in Ihrer IBM Spectrum Protect Plus-Umgebung finden Sie in den IBM Spectrum Protect Plus Blueprints.

Die folgende Liste enthält die Basiskomponenten von IBM Spectrum Protect Plus:

IBM Spectrum Protect Plus-Server
Diese Komponente verwaltet das gesamte System. Der Server besteht aus mehreren Katalogen, die verschiedene Aspekte des Systems überwachen, z. B. Zurückschreibungspunkte, Konfiguration, Berechtigungen und Anpassungen. Normalerweise gibt es eine einzige IBM Spectrum Protect Plus-Appliance in einer Implementierung, auch wenn die Implementierung auf mehrere Positionen verteilt ist.

Der IBM Spectrum Protect Plus-Server enthält einen integrierten vSnap-Server und einen VADP-Proxy-Server (VADP = VMware vStorage API for Data Protection). In kleinen Sicherungsumgebungen reichen diese Server möglicherweise aus. In großen Umgebungen könnten jedoch weitere Server erforderlich sein.

Mit dem integrierten vSnap-Server kann eine kleine Anzahl virtueller Maschinen gesichert und zurückgeschrieben und IBM Spectrum Protect Plus-Operationen können ausgewertet werden. Wenn Ihre Anforderungen bezüglich der Datensicherung und -zurückschreibung steigen, lässt sich Ihr vSnap-Speicher durch Hinzufügen externer vSnap-Server erweitern. Durch das Hinzufügen externer vSnap-Server in Ihrer Umgebung können Sie die Auslastung der IBM Spectrum Protect Plus-Appliance verringern.

Site
Diese Komponente ist ein IBM Spectrum Protect Plus-Richtlinienkonstrukt, das zur Steuerung der Datenplatzierung in der Umgebung verwendet wird. Eine Site kann eine physische Site, wie beispielsweise ein Datencenter, oder eine logische Site, wie beispielsweise eine Abteilung oder eine Organisation, sein. IBM Spectrum Protect Plus-Komponenten werden Sites zugeordnet, um Datenpfade einzugrenzen und zu optimieren. Eine Implementierung verfügt immer über mindestens eine Site pro physischer Position. Als Methode zur Eingrenzung der Datenversetzung auf Sites wird die Kombination aus vSnap-Servern und VADP-Proxy-Servern an einer einzigen Site bevorzugt. Die Platzierung von Sicherungsdaten an einer Site wird durch SLA-Richtlinien (SLA = Service-Level-Agreement) gesteuert.

vSnap-Server
Diese Komponente ist ein Plattenspeicherpool, der Daten zum Zweck des Datenschutzes oder der Datenwiederverwendung von Produktionssystemen empfängt. Der vSnap-Server besteht aus mindestens einer Platte und kann vertikal (Platten zur Erhöhung der Kapazität hinzufügen) oder horizontal (mehrere vSnap-Server zur Verbesserung der Gesamtleistung einführen) skaliert werden. Jede Site kann einen oder mehrere vSnap-Server umfassen.

© Copyright IBM Corp. 2017, 2019

vSnap-Pool
Diese Komponente ist die logische Anordnung von Platten zur Bildung eines Speicherbereichspools, der von der Komponente vSnap-Server verwendet wird. Diese Komponente wird auch als Speicherpool bezeichnet.

VADP-Proxy
Diese Komponente ist für das Versetzen von Daten aus vSphere-Datenspeichern zuständig, um Schutz für virtuelle VMware-Maschinen bereitzustellen, und ist nur für den Schutz von VMware-Ressourcen erforderlich. Jede Site kann einen oder mehrere VADP-Proxys enthalten.

Benutzerschnittstellen

IBM Spectrum Protect Plus stellt die folgenden Schnittstellen für Konfigurations-, Verwaltungs- und Überwachungstasks bereit:

IBM Spectrum Protect Plus-Benutzerschnittstelle
Die IBM Spectrum Protect Plus-Benutzerschnittstelle ist die primäre Schnittstelle für die Konfiguration, Verwaltung und Überwachung von Datenschutzoperationen.

Eine Schlüsselkomponente der Schnittstelle ist das Dashboard, das Übersichtsdaten zum Zustand Ihrer Umgebung bereitstellt. Weitere Informationen zum Dashboard finden Sie in „Produktdashboard" auf Seite 3.

Die Menüleiste in der Benutzerschnittstelle enthält folgende Einträge:

Alertsymbol 	Mit diesem Symbol wird das Fenster **Alerts** geöffnet. Weitere Informationen zu Alerts finden Sie in „Alerts" auf Seite 4.
Hilfesymbol 	Mit diesem Symbol wird das Onlinehilfesystem geöffnet.
Menü 'Benutzer'	In diesem Menü wird der Name des angemeldeten Benutzers angezeigt. Das Menü ermöglicht den Zugriff auf Produktinformationen und -dokumentation, auf Protokolle und die Option zur Abmeldung des Benutzers.

vSnap-Befehlszeilenschnittstelle
Die vSnap-Befehlszeilenschnittstelle ist eine sekundäre Schnittstelle für die Verwaltung einiger Tasks zum Schützen von Daten. Für den Zugriff auf die Befehlszeilenschnittstelle führen Sie den Befehl **vsnap** aus. Der Befehl kann von der Benutzer-ID `serveradmin` oder von einem beliebigen anderen Betriebssystembenutzer mit vSnap-Administratorberechtigungen aufgerufen werden.

Verwaltungskonsole
Die Verwaltungskonsole wird zur Installation von Software-Patches und -Updates und zur Ausführung anderer Verwaltungstask verwendet, z. B. zum Verwalten von Sicherheitszertifikaten, zum Starten und Stoppen von IBM Spectrum Protect Plus und zum Ändern der Zeitzone für die Anwendung.

Beispielimplementierung

Die folgende Abbildung zeigt IBM Spectrum Protect Plus, das an zwei aktiven Positionen implementiert ist. An jeder Position gibt es Bestand, der geschützt werden muss. Position 1 verfügt über einen vCenter-Server und zwei vSphere-Datencenter sowie einen Bestand an virtuellen Maschinen. Position 2 verfügt über ein einziges Datencenter und einen kleineren Bestand an virtuellen Maschinen.

Der IBM Spectrum Protect Plus-Server ist an nur einer der Sites implementiert. VADP-Proxys und vSnap-Server (mit den entsprechenden Platten) sind an jeder Site implementiert, um das Versetzen von Daten im Kontext der geschützten vSphere-Ressourcen einzugrenzen.

Zwischen den vSnap-Servern an den beiden Sites ist die bidirektionale Replikation konfiguriert.

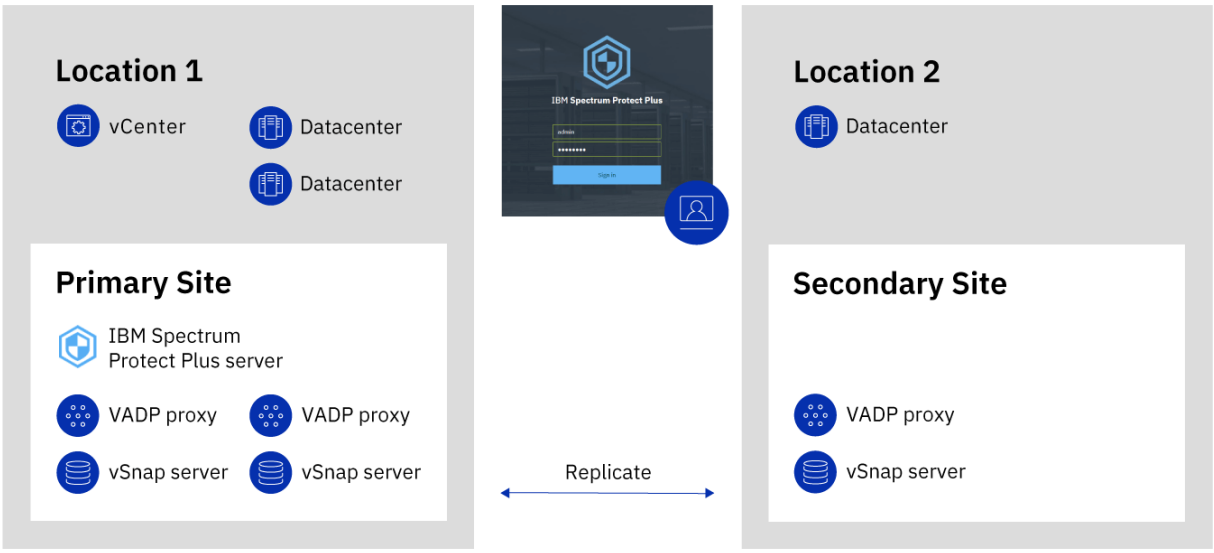


Abbildung 1. IBM Spectrum Protect Plus-Implementierung an zwei Standorten

Produktdashboard

Im IBM Spectrum Protect Plus-Dashboard wird eine Übersicht über den Zustand Ihrer virtuellen Umgebung in drei Abschnitten angezeigt: **Jobs und Operationen**, **Ziele** und **Abdeckung**.

Jobs und Operationen

Der Abschnitt **Jobs und Operationen** enthält eine Zusammenfassung der Jobaktivitäten über einen ausgewählten Zeitraum. Wählen Sie den Zeitraum in der Dropdown-Liste aus. In diesem Abschnitt werden die folgenden Informationen angezeigt:

Derzeit aktiv

Im Abschnitt **Derzeit aktiv** werden die Gesamtzahl der derzeit ausgeführten Jobs und der Prozentsatz der CPU-Auslastung in der virtuellen IBM Spectrum Protect Plus-Appliance angezeigt. Dieser Prozentsatz wird alle 10 Sekunden aktualisiert.

Um detaillierte Informationen zur Ausführung von Jobs anzuzeigen, klicken Sie auf **Anzeigen**.

Protokoll

Im Abschnitt **Protokoll** wird die Gesamtzahl der Jobs angezeigt, die innerhalb des ausgewählten Zeitraums ausgeführt wurden. Derzeit aktive Jobs werden hierbei nicht berücksichtigt.

In diesem Abschnitt wird darüber hinaus die Erfolgsquote für Jobs im ausgewählten Zeitraum angezeigt. Die Erfolgsquote wird mit der folgenden Formel berechnet:

100 x Erfolgreiche Jobs / Gesamtzahl der Jobs = Erfolgsquote

Beendete Jobs werden nach Jobstatus angezeigt:

Erfolgreich
Die Anzahl der Jobs, die ohne Warnungen oder kritische Fehler beendet wurden.

Fehlschlagen
Die Anzahl der Jobs, die wegen kritischer Fehler fehlgeschlagen sind oder die nicht beendet werden konnten.

Warnung
Die Anzahl der Jobs, die teilweise ausgeführt oder übersprungen wurden oder die sonstige Warnungen ausgelöst haben.

Um detaillierte Informationen zum Jobprotokoll anzuzeigen, klicken Sie auf **Anzeigen**.

Ziele

Im Abschnitt **Ziele** wird eine Zusammenfassung der Einheiten angezeigt, die für Sicherungsoperationen verwendet werden. In diesem Abschnitt werden die folgenden Informationen angezeigt:

Kapazitätszusammenfassung
Im Abschnitt **Kapazitätszusammenfassung** wird die aktuelle Auslastung und Verfügbarkeit der vSnap-Server angezeigt, die IBM Spectrum Protect Plus zur Verfügung stehen.

Um Informationen zu vSnap-Servern anzuzeigen, klicken Sie auf **Anzeigen**.

Einheitenstatus
Im Abschnitt **Einheitenstatus** wird die Gesamtzahl Einheiten angezeigt, die für die Verwendung verfügbar sind.

Die Anzahl Einheiten, die offline oder anderweitig nicht verfügbar sind, wird im Feld **Inaktiv** angezeigt.

Die Anzahl Einheiten, deren Kapazität ausgeschöpft ist, wird im Feld **Voll** angezeigt.

Datenreduktion
Im Abschnitt **Datenreduktion** werden das Datendeduplizierungsverhältnis und das Datenkomprimierungsverhältnis angezeigt.

Das Datendeduplizierungsverhältnis ist das geschützte Datenvolumen im Vergleich zu dem physischen Speicherbereich, der zum Speichern der Daten nach dem Entfernen von Duplikaten benötigt wird. Dieses Verhältnis gibt die Speicherbereichseinsparungen an, die zusätzlich zum Komprimierungsverhältnis erzielt werden. Wenn die Deduplizierung inaktiviert ist, ist das Verhältnis 1.

Abdeckung

Im Abschnitt **Abdeckung** werden eine Zusammenfassung der von IBM Spectrum Protect Plus inventarisierten Ressourcen sowie die SLA-Richtlinien (SLA = Service-Level-Agreement), die den Ressourcen zugeordnet sind, angezeigt. In diesem Abschnitt werden die folgenden Informationen angezeigt:

Quellenschutz
Im Abschnitt **Quellenschutz** wird die Gesamtzahl der im IBM Spectrum Protect Plus-Katalog inventarisierten Quellenressourcen (z. B. virtuelle Maschinen und Anwendungsserver) angezeigt. Die Anzahl der geschützten und der ungeschützten Ressourcen wird angezeigt.

In diesem Abschnitt wird auch das Verhältnis der in IBM Spectrum Protect Plus geschützten Ressourcen zur Gesamtzahl der Ressourcen in Prozent angezeigt.

Richtlinien
Im Abschnitt **Richtlinien** wird die Gesamtzahl der SLA-Richtlinien angezeigt, denen Schutzjobs zugeordnet sind.

In diesem Abschnitt werden auch die drei SLA-Richtlinien mit der höchsten Anzahl zugeordneter Ressourcen angezeigt.

Um detaillierte Informationen zu allen SLA-Richtlinien anzuzeigen, klicken Sie auf **Anzeigen**.

Alerts

Im Menü **Alerts** werden aktuelle und jüngste Warnungen und Fehler in der IBM Spectrum Protect Plus-Umgebung angezeigt. Die Anzahl der Alerts wird in einem roten Kreis angezeigt, was bedeutet, dass Alerts vorhanden sind und aufgerufen werden können.

Klicken Sie auf das Menü **Alerts**, um die Alertliste anzuzeigen. Jeder Listeneintrag verfügt über ein Statussymbol, eine Zusammenfassung des Alerts, eine Angabe der Zeit, zu der die zugehörige Warnung bzw. der zugehörige Fehler aufgetreten ist, und einen Link zum Aufrufen zugehöriger Protokolle.

Die Alertliste kann folgende Alerttypen enthalten:

Alerttypen

Job fehlgeschlagen
Wird angezeigt, wenn ein Job fehlschlägt.

Job teilweise erfolgreich
Wird angezeigt, wenn ein Job teilweise erfolgreich ausgeführt wird.

Unzureichender Systemplattenspeicherbereich
Wird angezeigt, wenn der freie Plattenspeicherbereich kleiner-gleich 10 % ist.

Unzureichender vSnap-Speicherbereich
Wird angezeigt, wenn der freie Plattenspeicherbereich kleiner-gleich 10 % ist.

Unzureichender Systemspeicher
Wird angezeigt, wenn die Speicherbelegung 95 % überschreitet.

Hohe CPU-Auslastung des Systems
Wird angezeigt, wenn die Prozessorauslastung 95 % überschreitet.

Hypervisor-VM nicht gefunden
Wird angezeigt, wenn die VM nicht gefunden wird.

Ausnahme für gesperrte Replikationsspeichermomentaufnahme
Wird angezeigt, wenn die Replikationsspeichermomentaufnahme gesperrt ist. Erhöhen Sie den Wert für die Replikationsaufbewahrung oder die Richtlinie für die Replikationshäufigkeit.

Ausnahme für gesperrte Auslagerungsspeichermomentaufnahme
Wird angezeigt, wenn die zuletzt ausgelagerte Speichermomentaufnahme gesperrt ist. Erhöhen Sie den Wert für die Auslagerungsaufbewahrung oder die Richtlinie für die Auslagerungshäufigkeit.

Fehlschlagen der SQL-Protokollsicherung
Wird angezeigt, wenn eine Protokollsicherung für eine Datenbank fehlschlägt.

Fehlschlagen der SQL-Protokoll-SMO-Sicherung
Wird angezeigt, wenn eine SMO-Transaktionsprotokollsicherung fehlschlägt.

Zu große SQL-Protokollgröße
Wird angezeigt, wenn die Transaktionsprotokollgröße den verfügbaren Speicherbereich auf der Platte überschreitet.

Unzureichender verbleibender Speicherbereich für SQL-Protokoll
Wird angezeigt, wenn der Plattenspeicherbereich für das Staging-Verzeichnis der Transaktionsprotokollsicherung unzureichend ist; zeigt den verbleibenden Speicherbereich an.

Rollenbasierte Zugriffssteuerung

Die rollenbasierte Zugriffssteuerung definiert die Ressourcen und Berechtigungen, die für IBM Spectrum Protect Plus-Benutzeraccounts zur Verfügung stehen.

Beim rollenbasierten Zugriff erhalten Benutzer ausschließlich Zugriff auf die von ihnen benötigten Funktionen und Ressourcen. Eine Rolle kann einem Benutzer beispielsweise erlauben, Sicherungs- und Zurückschreibungsjobs für Hypervisorressourcen auszuführen, aber nicht die Ausführung von Verwaltungstasks wie z. B. das Erstellen oder Ändern von Benutzeraccounts.

Damit ein Benutzer die in dieser Dokumentation beschriebenen Tasks ausführen kann, muss er zu einer Rolle gehören, die über die erforderlichen Berechtigungen verfügt. Stellen Sie sicher, dass Ihr Benutzeraccount zu einer Rolle gehört, die über die erforderlichen Berechtigungen verfügt, bevor Sie eine Task starten.

Informationen zur Definition und Verwaltung des Benutzerzugriffs finden Sie in Kapitel 13, „Benutzerzugriff verwalten”, auf Seite 311.

Sicherungsspeicherdaten replizieren

Wenn Sie die Replikation von Sicherungsdaten aktivieren, werden Daten eines vSnap-Servers auf einem anderen vSnap-Server asynchron repliziert. Sie können beispielsweise Sicherungsdaten eines vSnap-Servers an einer primären Site auf einem vSnap-Server an einer sekundären Site replizieren.

Replikation von Sicherungsspeicherdaten aktivieren

Gehen Sie wie folgt vor, um die Replikation von Sicherungsspeicherdaten zu aktivieren:

1. Richten Sie eine Replikationspartnerschaft zwischen vSnap-Servern ein. Replikationspartnerschaften werden im Fenster "Verwalten" eines registrierten vSnap-Servers erstellt. Wählen Sie im Abschnitt **Speicherpartner konfigurieren** einen anderen registrierten vSnap-Server als Speicherpartner aus, der als Ziel der Replikationsoperationen dienen soll.

   Stellen Sie sicher, dass der Pool auf dem Partnerserver so groß ist, dass er replizierte Daten aus dem Pool des primären Servers aufnehmen kann.
2. Aktivieren Sie die Replikation von Sicherungsspeicherdaten. Die Replikationsfunktion wird mithilfe von Sicherungsrichtlinien aktiviert, die auch als SLA-Richtlinien (SLA = Service-Level-Agreement) bezeichnet werden. Diese Richtlinien definieren Parameter, die auf Sicherungsjobs angewendet werden. Hierzu gehören die Häufigkeit von Sicherungsoperationen und die Aufbewahrungsrichtlinie für die Sicherungen. Weitere Informationen zu SLA-Richtlinien finden Sie in Kapitel 6, „SLA-Richtlinien für Sicherungsoperationen verwalten", auf Seite 93.

   Sie können die Optionen zur Sicherungsspeicherreplikation im Abschnitt **Operativer Schutz** > **Replikationsrichtlinie** einer SLA-Richtlinie definieren. Zu den Optionen gehören die Häufigkeit der Replikation, die Zielsite und die Aufbewahrung der Replikation.

Hinweise zur Aktivierung der Replikation von Sicherungsspeicherdaten

Lesen Sie die Hinweise zur Aktivierung der Replikation von Sicherungsspeicherdaten:

- Wenn es in Ihrer Umgebung eine Kombination aus verschlüsselten und nicht verschlüsselten vSnap-Servern gibt, wählen Sie **Nur verschlüsselten Plattenspeicher verwenden** aus, um Daten auf verschlüsselten vSnap-Servern zu replizieren. Wenn diese Option ausgewählt wird und keine verschlüsselten vSnap-Server verfügbar sind, schlägt der zugeordnete Job fehl.
- Für Eins-zu-viele-Replikationsszenarios, in denen eine einzelne Gruppe von Sicherungsdaten auf mehreren vSnap-Servern repliziert wird, erstellen Sie mehrere SLA-Richtlinien für jede Replikationssite.

In sekundären Sicherungsspeicher auslagern

Der vSnap-Server ist die primäre Sicherungsposition für Momentaufnahmen. Alle IBM Spectrum Protect Plus-Umgebungen verfügen über mindestens einen vSnap-Server. Wahlweise können Sie Momentaufnahmen aus einem vSnap-Server in sekundären Sicherungsspeicher auslagern.

Die folgenden sekundären Sicherungsspeicherziele sind für Auslagerungsoperationen verfügbar:

- IBM Cloud Object Storage (einschließlich IBM Cloud Object Storage Systems)
- Amazon Simple Storage Service (Amazon S3)
- Microsoft Azure
- Repository-Server (im aktuellen Release von IBM Spectrum Protect Plus muss der Repository-Server ein IBM Spectrum Protect-Server sein)

Diese Ziele unterstützen die folgenden Speichertypen. Der verwendete Speichertyp ist von Faktoren wie Ihrer Wiederherstellungszeit und Sicherheitszielen abhängig.

Objektspeicher

Objektspeicher ist eine Methode zum Speichern von Daten, bei der Daten als diskrete Einheiten (oder Objekte) in einem Speicherpool oder Repository gespeichert werden, der bzw. das keine Dateihierarchie verwendet, sondern alle Daten auf derselben Ebene speichert.

Objektspeicher ist eine Option, wenn Daten auf einen IBM Spectrum Protect-Server oder in ein Cloudspeichersystem ausgelagert werden sollen. Wenn Momentaufnahmedaten in Objektspeicher ausgelagert werden, wird während der ersten Auslagerungsoperation eine vollständige Kopie erstellt. Nachfolgende Kopien sind inkrementell und erfassen kumulative Änderungen, die seit der letzten Auslagerung erfolgt sind.

Die Auslagerung von Momentaufnahmen in Objektspeicher ist geeignet, wenn relativ kurze Sicherungs- und Wiederherstellungszeiten erzielt werden sollen, ohne dass die Vorteile hinsichtlich längerfristigem Schutz, Kosten und Sicherheit, die Band- oder Cloudarchivierungsspeicher bieten, erforderlich wären.

Band- oder Cloudarchivierungsspeicher

Bandspeicher bedeutet, dass Daten auf physischen Banddatenträgern oder in einem virtuellen Bandarchiv gespeichert werden. Bandspeicher ist eine Option, wenn Daten auf einen IBM Spectrum Protect-Server ausgelagert werden sollen. Durch die Speicherung auf Banddatenträgern an einem sicheren anderen Standort, der nicht mit dem Internet verbunden ist, können Sie Ihre Daten vor Onlinebedrohungen, wie Malware und Hackern, schützen.

Cloudarchivierungsspeicher ist eine Methode zur langfristigen Speicherung, bei der Daten in einen der folgenden Speicherservices kopiert werden: Amazon Glacier, IBM Cloud Object Storage-Archivtier oder Microsoft Azure-Archiv.

Wenn Sie Daten auf Band oder in ein Cloudspeichersystem auslagern, wird eine vollständige Kopie der Daten erstellt.

Die Auslagerung von Momentaufnahmen in Band- oder Cloudarchivierungsspeicher bietet zusätzliche Vorteile hinsichtlich Kosten und Sicherheit. Da die Auslagerung in diese Speichertypen jedoch eine vollständige Datenkopie erfordert, verlängert sich die zum Kopieren der Daten erforderliche Zeit. Darüber hinaus ist die Wiederherstellungszeit nicht vorhersehbar und die Verarbeitung der Daten kann länger dauern, bevor sie verwendbar sind.

Informationen zum Kopieren von Momentaufnahmedaten in Objektspeicher und Archivierungsspeicher für das jeweilige Cloudspeichersystem finden Sie in „Cloudanforderungen” auf Seite 20.

Sekundären Sicherungsspeicher hinzufügen und Sicherungsrichtlinien erstellen

Für die Auslagerung von Daten in sekundären Speicher sind folgende Aktionen erforderlich:

Aktion	Vorgehensweise
Gehen Sie zum Auslagern von Daten auf einen Repository-Server wie folgt vor: • Definieren Sie IBM Spectrum Protect Plus als Objektclient in der IBM Spectrum Protect-Serverumgebung. • Fügen Sie den Speicher in IBM Spectrum Protect Plus hinzu.	Siehe „IBM Spectrum Protect-Server-Server als Auslagerungsziel konfigurieren” auf Seite 274 und „Repository-Server als Sicherungsspeicherprovider hinzufügen” auf Seite 279.
Fügen Sie zum Auslagern von Daten in den Cloudspeicher den Speicher in IBM Spectrum Protect Plus hinzu.	Führen Sie die Anweisungen für den ausgewählten Speichertyp aus: • „Amazon S3-Cloudspeicher als Sicherungsspeicherprovider hinzufügen” auf Seite 269 • „IBM Cloud Object Storage als Sicherungsspeicherprovider hinzufügen” auf Seite 270 • „Microsoft Azure-Cloudspeicher als Sicherungsspeicherprovider hinzufügen” auf Seite 272 • „Repository-Server als Sicherungsspeicherprovider hinzufügen” auf Seite 279
Erstellen Sie eine Sicherungsrichtlinie, die den Speicher enthält.	Siehe „Sicherungsrichtlinien erstellen” auf Seite 75.

Beispielimplementierungen

Die folgende Abbildung zeigt IBM Spectrum Protect Plus, das an zwei aktiven Positionen implementiert ist. An jeder Position gibt es Bestand, der geschützt werden muss. Position 1 verfügt über einen vCenter-

Server und zwei vSphere-Datencenter sowie einen Bestand an virtuellen Maschinen. Position 2 verfügt über ein einziges Datencenter und einen kleineren Bestand an virtuellen Maschinen.

Der IBM Spectrum Protect Plus-Server ist an nur einer der Sites implementiert. VADP-Proxys und vSnap-Server (mit den entsprechenden Platten) sind an jeder Site implementiert, um das Versetzen von Daten im Kontext der geschützten vSphere-Ressourcen einzugrenzen.

Zwischen den vSnap-Servern an den beiden Sites ist die bidirektionale Replikation konfiguriert.

Für langfristigen Datenschutz werden Momentaufnahmen aus dem vSnap-Server an der sekundären Site in den Cloudspeicher ausgelagert.

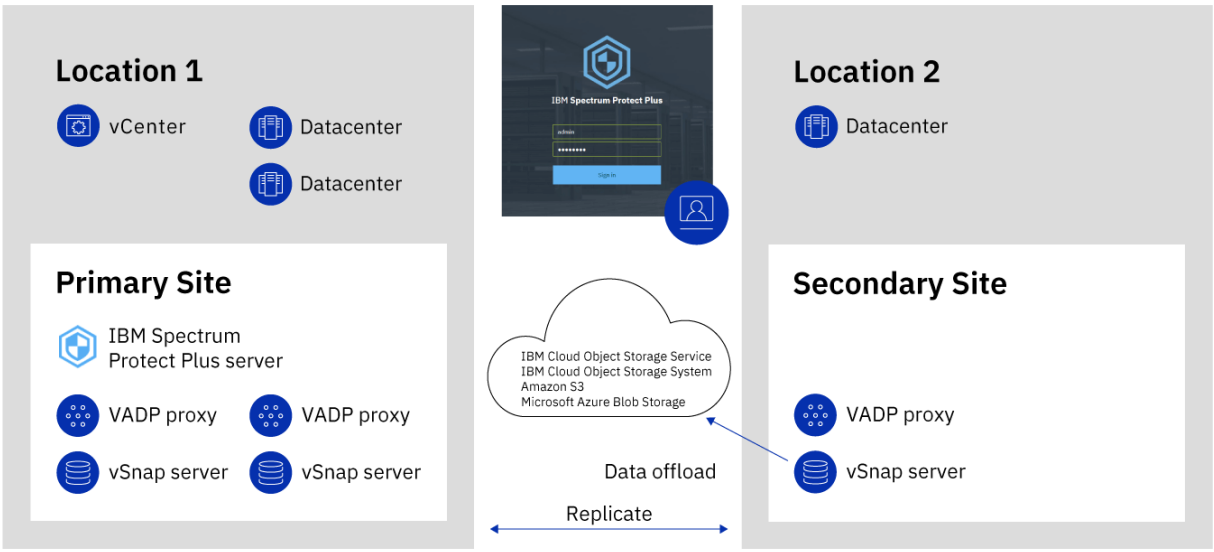


Abbildung 2. IBM Spectrum Protect Plus-Implementierung an zwei Standorten mit Auslagerung in Cloud-speicher

Die folgende Abbildung zeigt dieselbe Implementierung wie die vorherige Abbildung.

In dieser Implementierung werden Momentaufnahmen jedoch für langfristigen Datenschutz aus dem vSnap-Server an der sekundären Site nach IBM Spectrum Protect ausgelagert.

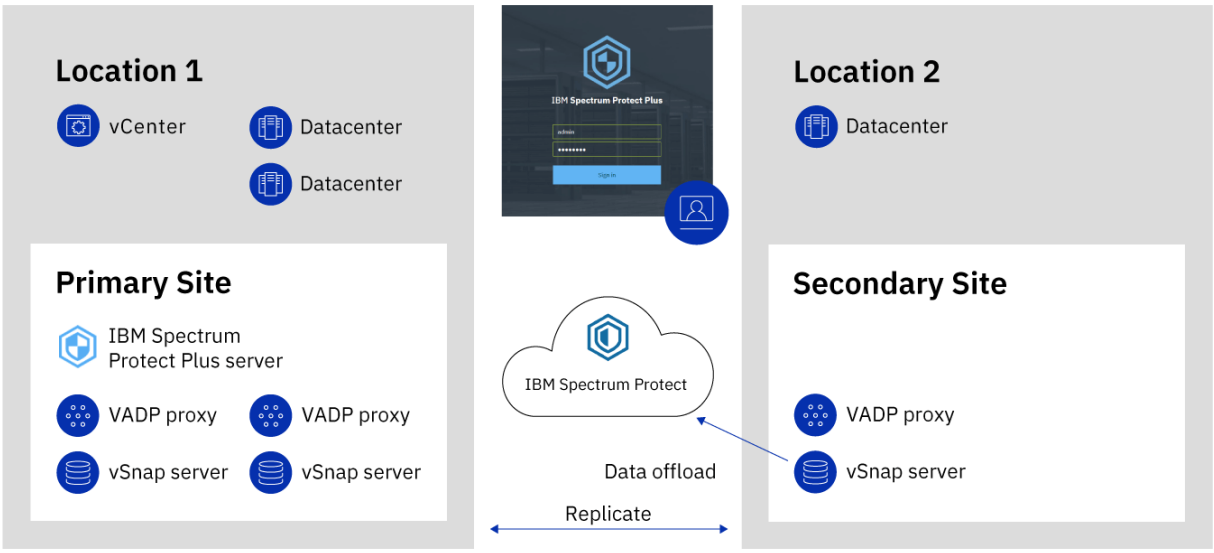


Abbildung 3. IBM Spectrum Protect Plus-Implementierung an zwei Standorten mit Auslagerung nach IBM Spectrum Protect

IBM Spectrum Protect Plus on IBM Cloud

IBM Spectrum Protect Plus ist als IBM Cloud for VMware Solutions-Service, IBM Spectrum Protect Plus on IBM Cloud, verfügbar.

Mit IBM Cloud for VMware Solutions können Sie Ihre lokalen VMware-Workloads mithilfe der skalierbaren IBM Cloud-Infrastruktur und der VMware-Hybridvirtualisierungstechnologie in IBM Cloud integrieren oder migrieren.

Die wichtigsten Vorteile von IBM Cloud for VMware Solutions sind:

Globale Reichweite
Sie können Ihre Hybrid-Cloud-Speicheranforderungen auf maximal 30 IBM Cloud-Datencenter auf Unternehmensebene weltweit erweitern.

Optimierte Integration
Verwenden Sie den optimierten Prozess für die Integration der Hybrid-Cloud in die IBM Cloud-Infrastruktur.

Automatisierte Implementierung und Konfiguration
Sie können eine auf Unternehmen abgestimmte VMware-Umgebung mit bedarfsgesteuerten IBM Cloud-Bare-Metal-Servern und virtuellen Servern mithilfe der automatisierten Implementierung und Konfiguration der VMware-Umgebung implementieren.

Vereinfachung
Sie können eine VMware-Cloudplattform verwenden, ohne die zugrunde liegende physische Rechen-, Speicher- und Netzinfrastruktur sowie Softwarelizenzen anzugeben, zu beschaffen, zu implementieren und zu verwalten.

Erweiterungs- und Verminderungsflexibilität
Sie können Ihre VMware-Workloads Ihren Geschäftsanforderungen entsprechend erweitern oder vermindern.

Einzelne Verwaltungskonsole
Sie verwenden eine einzelne Konsole, um die VMware-Umgebungen in IBM Cloud zu implementieren, um darauf zuzugreifen und um sie zu verwalten.

Verfügbare Funktionen in IBM Spectrum Protect Plus on IBM Cloud

IBM Spectrum Protect Plus unterstützt sowohl VMware- als auch Microsoft Hyper-V-Umgebungen.

IBM Spectrum Protect Plus on IBM Cloud unterstützt jedoch nur VMware-Umgebungen.

Diese Dokumentation enthält Themen zu Hyper-V-spezifischen Funktionen. Wenn Sie IBM Spectrum Protect Plus on IBM Cloud verwenden, stehen diese Funktionen nicht zur Verfügung.

Die aktuellen Versionen von IBM Spectrum Protect Plus und IBM Spectrum Protect Plus on IBM Cloud stimmen möglicherweise nicht überein. Rufen Sie die Onlineproduktdokumentation auf und wählen Sie die Produktversion aus, um die Dokumentation für die verwendete Version von IBM Spectrum Protect Plus on IBM Cloud zu suchen.

Weitere Informationen

Informationen zur Bestellung, Installation und Konfiguration von IBM Spectrum Protect Plus on IBM Cloud finden Sie in der folgenden Dokumentation. Für den Zugriff auf die Dokumentation benötigen Sie eine IBMid.

- Getting started with IBM Cloud for VMware Solutions
- Components and considerations for IBM Spectrum Protect Plus on IBM Cloud
- Managing IBM Spectrum Protect Plus on IBM Cloud

IBM Spectrum Protect Plus auf der AWS-Cloudplattform

IBM Spectrum Protect Plus auf der Amazon Web Services-(AWS-)Cloudplattform ist eine Lösung für Benutzer, die IBM Spectrum Protect Plus lokal ausführen, aber Datenbanken, die in der AWS-Cloud ausgeführt werden, schützen möchten.

IBM Spectrum Protect Plus on AWS ist eine Hybridlösung, bei der der IBM Spectrum Protect Plus-Server lokal vorhanden ist und sich der vSnap-Server auf AWS befindet.

Die Richtlinie, die Systemverwaltung und die Zugriffssteuerung sowie andere Funktionen von IBM Spectrum Protect Plus werden vom IBM Spectrum Protect Plus-On-Premises-Server verwaltet. Daten aus Datenbanken auf AWS werden dann in dem vSnap-Server gespeichert, der sich ebenfalls auf AWS befindet.

IBM Spectrum Protect Plus auf AWS implementieren

Auf der IBM Spectrum Protect Plus-Seite unter AWS Marketplace werden die AWS CloudFormation-Schablonen, die zum Implementieren des vSnap-Servers auf AWS erforderlich sind, zusammen mit Preisen, Einsatzmöglichkeiten und Unterstützungsinformationen bereitgestellt. Befolgen Sie die Anweisungen auf dieser Seite und im IBM Spectrum Protect Plus on the AWS Cloud Deployment Guide, um Ihre On-Premises- und AWS-Umgebungen zu konfigurieren.

Die IBM Spectrum Protect Plus on AWS-Implementierung schließt IBM Spectrum Protect Plus Version 10.1.3 ein. Soll die aktuelle Version von IBM Spectrum Protect Plus verwendet werden, befolgen Sie die Anweisungen in Kapitel 5, „IBM Spectrum Protect Plus-Komponenten aktualisieren”, auf Seite 87, um ein Upgrade durchzuführen.

Kapitel 2. IBM Spectrum Protect Plus installieren

Lesen Sie vor der Installation von IBM Spectrum Protect Plus die Informationen zu den Systemanforderungen und Installationsprozeduren.

Roadmap für die Produktimplementierung

Folgen Sie der Roadmap, um IBM Spectrum Protect Plus zu installieren, zu konfigurieren und zu verwenden.

Aktion	Vorgehensweise
Sicherstellen, dass Ihre Systemumgebung die Hardware- und Softwareanforderungen erfüllt.	Siehe „Systemanforderungen” auf Seite 11.
Feststellen, wie in Ihrer IBM Spectrum Protect Plus-Umgebung die Anzahl Komponenten festgelegt wird und wie Komponenten erstellt und integriert werden.	Siehe IBM Spectrum Protect Plus Blueprints.
IBM Spectrum Protect Plus installieren.	Siehe Kapitel 2, „IBM Spectrum Protect Plus installieren”, auf Seite 11.
Zusätzliche vSnap-Server installieren und konfigurieren, falls diese Server zur Unterstützung Ihrer Umgebung erforderlich sind.	Siehe Kapitel 3, „vSnap-Server installieren und konfigurieren”, auf Seite 55.
Zusätzliche VADP-Proxys erstellen und konfigurieren, falls diese Proxys zur Unterstützung Ihrer Umgebung erforderlich sind (VADP = VMware vStorage API for Data Protection).	Siehe „VADP-Sicherungsproxys verwalten” auf Seite 112.
Die grundlegenden Schritte für die Konfiguration von IBM Spectrum Protect Plus und den Einstieg zur Verwendung des Produkts ausführen.	Siehe Kapitel 4, „Schnelleinstieg”, auf Seite 71.

Systemanforderungen

Informieren Sie sich vor der Installation von IBM Spectrum Protect Plus über die Hardware- und Softwareanforderungen für die Produktkomponenten und anderen Komponenten, deren Installation in der Speicherumgebung geplant ist.

Um sicherzustellen, dass Sicherungs- und Zurückschreibungsoperationen erfolgreich ausgeführt werden können, muss Ihr System die Hardware- und Softwareanforderungen erfüllen. Die folgenden Anforderungen dienen als Ausgangspunkt. Die aktuellen Anforderungen, die unter Umständen Aktualisierungen umfassen, finden Sie in Technote 2013790.

Informationen darüber, wie Sie in Ihrer IBM Spectrum Protect Plus-Umgebung die Anzahl Komponenten festlegen sowie Komponenten erstellen und integrieren, die in Ihren Spezifikationen aufgelistet sind, finden Sie in den IBM Spectrum Protect Plus Blueprints.

Komponentenanforderungen

Stellen Sie sicher, dass Sie über die erforderliche Systemkonfiguration und einen unterstützten Browser verfügen, um IBM Spectrum Protect Plus implementieren und ausführen zu können.

Um sicherzustellen, dass Sicherungs- und Zurückschreibungsoperationen erfolgreich ausgeführt werden können, muss Ihr System die Hardware- und Softwareanforderungen erfüllen. Die folgenden Anforderun-

© Copyright IBM Corp. 2017, 2019

gen dienen als Ausgangspunkt. Die aktuellen Anforderungen, die unter Umständen Aktualisierungen umfassen, finden Sie in Technote 2013790.

IBM Spectrum Protect Plus-Unterstützung für Plattformen anderer Anbieter, Anwendungen, Services und Hardwareparalleleinheiten anderer Anbieter. Wenn für ein Produkt oder eine Version eines anderen Anbieters erweiterte Unterstützung, Self-Service-Unterstützung oder Unterstützung für das Ende des Lebenszyklus bereitgestellt wird, unterstützt IBM Spectrum Protect Plus dies auf derselben Ebene.

Installation der virtuellen Maschine

IBM Spectrum Protect Plus wird als eine virtuelle Appliance installiert. Bevor Sie IBM Spectrum Protect Plus auf dem Host implementieren, müssen Sie sicherstellen, dass die folgenden Anforderungen erfüllt sind:

- vSphere 5.5, 6.0, 6.5 oder 6.7
- Microsoft Hyper-V Server 2016 oder Hyper-V 2019

Konfigurieren Sie für die Erstimplementierung Ihre virtuelle Appliance so, dass sie die folgenden Mindestanforderungen erfüllt:

- 64-Bit-Maschine mit 8 Kernen
- 48 GB Speicher
- 536 GB Plattenspeicher für die virtuelle Maschine

Verwenden Sie einen NTP-Server, um die Zeitzonen für IBM Spectrum Protect Plus-Ressourcen in Ihrer Umgebung (wie beispielsweise die virtuelle IBM Spectrum Protect Plus-Appliance, Speicherarrays, Hypervisoren und Anwendungsserver) zu synchronisieren. Wenn die Systemzeiten auf den einzelnen Systemen deutlich voneinander abweichen, können während der Anwendungsregistrierung, dem Katalogisieren von Metadaten, Bestands-, Sicherungs-, Zurückschreibungs- oder Dateizurückschreibungsjobs Fehler auftreten. Weitere Informationen zum Erkennen und Korrigieren von Zeitabweichungen enthält der folgende Artikel in der VMware-Knowledge Base: Time in virtual machine drifts due to hardware timer drift.

Browserunterstützung

Führen Sie IBM Spectrum Protect Plus auf einem Computer aus, der Zugriff auf die installierte virtuelle Appliance hat. IBM Spectrum Protect Plus wurde für die folgenden Web-Browser getestet. Beachten Sie, dass möglicherweise auch höhere Browserversionen unterstützt werden.

- Firefox 55.0.3
- Google Chrome 60.0.3112 und höher
- Microsoft Edge 40.15063/Microsoft EdgeHTML 15.15063 und höher

Wenn Ihre Bildschirmauflösung unter 1024 x 768 Pixel liegt, passen einige Elemente möglicherweise nicht in das Fenster. Popup-Fenster müssen in Ihrem Browser aktiviert sein, um auf das Hilfesystem und einige IBM Spectrum Protect Plus-Operationen zugreifen zu können.

IBM Spectrum Protect-Anforderungen

Wenn geplant ist, IBM Spectrum Protect als einen Repository-Server für Cloudauslagerungsoperationen zu verwenden, stellen Sie sicher, dass IBM Spectrum Protect Version 8.1.8 verwendet wird.

IBM Spectrum Protect Plus-Ports

Die folgenden Ports werden von IBM Spectrum Protect Plus und zugehörigen Services verwendet. Ports, die in der Spalte "Firewallregel" mit "Accept" angegeben sind, verwenden sichere Verbindungen (HTTPS oder SSL).

Tabelle 1. Eingehende Firewallverbindungen (IBM Spectrum Protect Plus-Appliance)

Port	Protokoll	Firewall	Service	Beschreibung
22	TCP	Accept	OpenSSH 5.3 (Protokoll 2.0)	Für die Fehlerbehebung in IBM Spectrum Protect Plus verwendet
443	TCP	Accept	Ein Mikroservice, der einen Reverse Proxy ausführt	Haupteingangspunkt für die Clientverbindungen (SSL)
5671	TCP, AMQP	Accept	RabbitMQ	Nachrichtenframework zum Verwalten von Nachrichten, die von den VADP-Proxy- und VMware-Jobverwaltungsworkern erstellt und verarbeitet werden. Erleichtert außerdem die Verwaltung von Jobprotokollen.
8090	TCP	Accept	Administrative Console Framework (ACF)	Erweiterbares Framework für Systemverwaltungsfunktionen. Unterstützt Plug-ins, die Operationen wie Systemaktualisierungen und Katalogsicherungs- oder -zurückschreibungsoperationen ausführen.
8761	TCP	Accept	Discovery Server	Erkennt automatisch VADP-Proxys und wird von IBM Spectrum Protect Plus-VM-Sicherungsoperationen verwendet.

Tabelle 2. Eingehende Firewallverbindungen (integrierter vSnap-Server)

Port	Protokoll	Firewall	Service	Beschreibung
111	TCP	Accept	RPC Port Bind	Ermöglicht Clients das Erkennen von Ports, die ONC-Clients (ONC = Open Network Computing) für die Kommunikation mit ONC-Servern (intern) erfordern.
2049	TCP	Accept	NFS	Für die NFS-Datenübertragung zu und von vSnap (intern) verwendet
3260	TCP	Accept	iSCSI	Für die iSCSI-Datenübertragung zu und von vSnap (intern) verwendet
20048	TCP	Accept	NFS	Für die NFS-Datenübertragung zu und von vSnap (intern) verwendet

Tabelle 3. Abgehende Firewallverbindungen (IBM Spectrum Protect Plus)

Port	Protokoll	Service	Beschreibung
22	TCP	OpenSSH 5.3 (Protokoll 2.0)	Für die SSH-Kommunikation zu fernen Servern, die Gastanwendungskomponenten ausführen, verwendet.
25	TCP	SMTP	E-Mail-Service
389	TCP	LDAP	Active Directory-Dienste
443	TCP	VMware ESXi Host	ESXi-Host-Port für die Verwaltung von Operationen
443	TCP	VMware vCenter	Clientverbindungen zu vCenter
636	TCP	LDAP	Active Directory-Dienste (SSL)

Tabelle 3. Abgehende Firewallverbindungen (IBM Spectrum Protect Plus) (Forts.)			
Port	**Protokoll**	**Service**	**Beschreibung**
902	TCP	VMware NFC	Network File Copy (NFC) stellt einen dateitypsensitiven FTP-Service für vSphere-Komponenten zur Verfügung. Standardmäßig verwendet ESXi NFC für Operationen wie das Kopieren und Versetzen von Daten zwischen Datenspeichern.
5985	TCP	Windows-Remoteverwaltung (WinRM)	Clientverbindungen für Hyper-V- und Gastanwendungen
8098	TCP	VADP-Proxy	Datenschutzproxy der virtuellen Maschine
8900	TCP	vSnap	OVA-/Installationsprogrammversion des intelligenten Speicherframeworks, das als Ziel für Datenschutzoperationen verwendet wird.

vSnap-Server-Anforderungen

Ein vSnap-Server ist das primäre Sicherungsziel für IBM Spectrum Protect Plus. In einer VMware- oder Hyper-V-Umgebung wird ein einzelner vSnap-Server mit dem Namen `localhost` automatisch zu dem Zeitpunkt der Erstimplementierung der virtuellen IBM Spectrum Protect Plus-Appliance installiert. In umfangreicheren Unternehmenssicherungsumgebungen sind unter Umständen weitere vSnap-Server erforderlich.

Ordnen Sie Speicher auf der Basis der Sicherungskapazität für eine effizientere Deduplizierung zu. Weitere Informationen und eine Anleitung zur Kapazitätsermittlung finden Sie in den IBM Spectrum Protect Plus Blueprints.

Stellen Sie bei der Erstimplementierung sicher, dass Ihre virtuelle Maschine oder physische Linux-Maschine die folgenden Mindestanforderungen erfüllt:

- 64-Bit-Prozessor mit 8 Kernen
- 32 GB Speicher
- 16 GB freier Speicherbereich im Stammdateisystem
- 128 GB freier Speicherbereich in einem anderen Dateisystem, das an der folgenden Position bereitgestellt wurde: `/opt/vsnap-data`

Der Linux-Netzmanagementservice muss installiert und aktiv sein.

Wahlweise ein Solid-State-Laufwerk (SSD) zur Verbesserung der Sicherungs- und Zurückschreibungsleistung

- Um die Sicherungsleistung zu verbessern, konfigurieren Sie den Pool für die Verwendung einer oder mehrerer Protokolleinheiten, die von einem SSD gesichert werden. Geben Sie mindestens zwei Protokolleinheiten an, um ein gespiegeltes Protokoll für bessere Redundanz zu erstellen.
- Um die Zurückschreibungsleistung zu verbessern, konfigurieren Sie den Pool für die Verwendung einer Cacheeinheit, die von einem SSD gesichert wird.

Installationsanforderungen für die virtuelle Maschine des vSnap-Servers

Bevor Sie den vSnap-Server auf dem Host implementieren, müssen Sie sicherstellen, dass die folgenden Anforderungen erfüllt sind:

- vSphere 5.5, 6.0, 6.5 oder 6.7
- Microsoft Hyper-V 2016 oder Microsoft Hyper-V 2019

Installationsanforderungen für den physischen vSnap-Server

Ab Version 10.1.3 stellt IBM Spectrum Protect Plus Funktionalität bereit, die die in RHEL 7.5 und CentOS 7.5 unterstützten Kernel-Level erfordert. Wenn Sie frühere Betriebssystemversionen als RHEL 7.5 und CentOS 7.5 verwenden müssen, verwenden Sie IBM Spectrum Protect Plus Version 10.1.2 für Installationen des physischen vSnap-Servers der Version 10.1.2.

Die folgenden Linux-Betriebssysteme werden für IBM Spectrum Protect Plus Version 10.1.4 oder höher für Installationen des physischen vSnap-Servers unterstützt:

- CentOS 7.1804 (7.5) (x86_64)
- CentOS 7.1810 (7.6) (x86_64)
- Red Hat Enterprise Linux 7.5 (x86_64)
- Red Hat Enterprise Linux 7.6 (x86_64)

Wenn Sie die folgenden Betriebssysteme verwenden, verwenden Sie IBM Spectrum Protect Plus Version 10.1.2 für Installationen des physischen vSnap-Servers der Version 10.1.2:

- CentOS Linux 7.3.1611 (x86_64)
- CentOS Linux 7.4.1708 (x86_64)
- Red Hat Enterprise Linux 7.3 (x86_64)
- Red Hat Enterprise Linux 7.4 (x86_64)

vSnap-Server-Ports

Die folgenden Ports werden von vSnap-Servern verwendet. Ports, die in der Spalte "Firewallregel" mit "Accept" angegeben sind, verwenden sichere Verbindungen (HTTPS oder SSL).

Tabelle 4. Eingehende vSnap-Firewallverbindungen

Port	Protokoll	Firewall	Service	Beschreibung
22	TCP	Accept	SSH	Für die Fehlerbehebung von vSnap-Servern verwendet
111	TCP	Accept	RPC Port Bind	Ermöglicht Clients das Erkennen von Ports, die ONC-Clients (ONC = Open Network Computing) für die Kommunikation mit ONC-Servern (intern) erfordern

Tabelle 4. Eingehende vSnap-Firewallverbindungen (Forts.)				
Port	**Protokoll**	**Firewall**	**Service**	**Beschreibung**
137	UDP	Accept	SMB/CIFS	Für die SMB- oder CIFS-Datenübertragung zu und von vSnap-Servern (intern) verwendet
138	UDP	Accept	SMB/CIFS	Für die SMB- oder CIFS-Datenübertragung zu und von vSnap-Servern (intern) verwendet
139	TCP	Accept	SMB/CIFS	Für die SMB- oder CIFS-Datenübertragung zu und von vSnap-Servern (intern) verwendet
445	TCP	Accept	SMB/CIFS	Für die SMB- oder CIFS-Datenübertragung zu und von vSnap-Servern (intern) verwendet
2049	TCP	Accept	NFS	Für die NFS-Datenübertragung zu und von vSnap-Servern (intern) verwendet
3260	TCP	Accept	iSCSI	Für die iSCSI-Datenübertragung zu und von vSnap-Servern (intern) verwendet
8900	TCP	Accept	HTTPS	vSnap-Server-REST-APIs
20048	TCP	Accept	NFS	Für die NFS-Datenübertragung zu und von vSnap-Servern (intern) verwendet

VADP-Proxy-Anforderungen

In IBM Spectrum Protect Plus kann sich die Ausführung von Sicherungsjobs für virtuelle Maschinen über VADP auf Systemressourcen auswirken. Durch die Erstellung von VADP-Sicherungsjobproxys ermöglichen Sie Lastverteilung und Lastausgleich für Ihre IBM Spectrum Protect Plus-Sicherungsjobs. Wenn Proxys vorhanden sind, wird die gesamte Verarbeitungslast von der IBM Spectrum Protect Plus-Appliance auf die Proxys verlagert.

Diese Funktion wurde nur für SUSE Linux Enterprise Server- und Red Hat-Umgebungen getestet. Die Funktion wird nur in 64-Bit-4-Kern-Konfigurationen oder höheren Konfigurationen mit einem Mindestkernel von 2.6.32 unterstützt.

VADP-Proxys unterstützen die folgenden VMware-Transportmodi: File, SAN, HotAdd, NBDSSL und NBD. Weitere Informationen zu VMware-Transportmodi finden Sie in Virtual Disk Transport Methods.

Diese Funktion wird nur in 64-Bit-4-Kern-Konfigurationen oder höheren Konfigurationen in den folgenden Linux-Umgebungen unterstützt:

- CentOS Linux 6.5 und höhere Wartungs- und Modifikationsstufen (ab 10.1.1 Patch 1)
- CentOS Linux 7.0 und höhere Wartungs- und Modifikationsstufen (ab 10.1.1 Patch 1)
- Red Hat Enterprise Linux 6, Fixpack 4 und höhere Wartungs- und Modifikationsstufen
- Red Hat Enterprise Linux 7 und höhere Wartungs- und Modifikationsstufen
- SUSE Linux Enterprise Server 12 und höhere Wartungs- und Modifikationsstufen

Weitere Informationen und eine Anleitung zur Kapazitätsermittlung finden Sie in den IBM Spectrum Protect Plus Blueprints.

Stellen Sie bei der Erstimplementierung eines VADP-Proxy-Servers sicher, dass Ihre Linux-Maschine die folgenden Mindestanforderungen erfüllt:

- 64-Bit-4-Kern-Prozessor
- 8 GB RAM erforderlich, bevorzugt 16 GB
- 60 GB freier Plattenspeicherbereich

Die Erhöhung der verwendeten CPUs und der gemeinsame Zugriff auf den VADP-Proxy-Server erfordern die entsprechende Erhöhung des Speichers, der auf dem Proxy-Server zugeordnet ist.

Der Proxy muss NFS-Dateisysteme bereitstellen können; dies erfordert in vielen Fällen die Installation eines NFS-Clientpakets. Die exakten Paketdetails sind abhängig von der Distribution unterschiedlich.

Jeder Proxy muss über einen vollständig qualifizierten Domänennamen verfügen, diesen auflösen können und vCenter erreichen können. vSnap-Server müssen vom Proxy erreichbar sein. Port 8098 auf dem VADP-Proxy-Server muss offen sein, wenn die Proxy-Server-Firewall aktiviert wird.

VADP-Proxy-Ports

Die folgenden Ports werden von VADP-Proxys verwendet. Ports, die in der Spalte "Firewallregel" mit "Accept" angegeben sind, verwenden sichere Verbindungen (HTTPS oder SSL).

Tabelle 5. Eingangs- VADP-Proxy-Firewallverbindungen

Port	Protokoll	Firewall	Service	Beschreibung
22	TCP	Accept	SSH	Port 22 wird verwendet, um den VADP-Proxy mit einer Push-Operation auf den Hostknoten zu übertragen.
8098	TCP	Accept	VADP	Standardport für die TLS-basierte REST-API-Kommunikation zwischen dem IBM Spectrum Protect Plus-Server und dem VADP-Proxy

Tabelle 6. Abgehende VADP-Proxy-Firewallverbindungen

Port	Protokoll	Service	Beschreibung
111	TCP	vSnap RPC Port Bind	Ermöglicht Clients das Erkennen von Ports, die ONC-Clients für die Kommunikation mit ONC-Servern (intern) erfordern.
443	TCP	VMware ESXi Host/ vCenter	Clientverbindungen zu vCenter
902	TCP	VMware ESXi Host	Network File Copy (NFC) stellt einen dateitypsensitiven FTP-Service für vSphere-Komponenten zur Verfügung. ESXi verwendet NFC standardmäßig für Operationen wie das Kopieren und Versetzen von Daten zwischen Datenspeichern.
2049	TCP	vSnap NFS	Für die NFS-Dateifreigabe mithilfe des vSnap-Servers verwendet.
5671	TCP	RabbitMQ	Nachrichtenframework zum Verwalten von Nachrichten, die von den VADP-Proxy- und VMware-Jobverwaltungsworkern erstellt und verarbeitet werden. Vereinfacht außerdem das Jobprotokoll.
8761	TCP	Discovery Server	Erkennt automatisch VADP-Proxys und wird von IBM Spectrum Protect Plus-VM-Sicherungsoperationen verwendet.
20048	TCP	vSnap mount	Stellt vSnap-Dateisysteme auf Clients, wie beispielsweise dem VADP-Proxy, Anwendungsservern und Virtualisierungsdatenspeichern, bereit.

Tipp: VADP-Proxys können mit einer Push-Operation auf Linux-basierte Server über SSH-Port 22 übertragen und auf diesen installiert werden.

Wenn das Firewallbefehlsscript auf Ihrem System nicht verfügbar ist, editieren Sie die Firewall manuell, um die erforderlichen Ports hinzuzufügen, und starten Sie die Firewall erneut. Weitere Informationen zum Editieren von Firewallregeln finden Sie in „Firewall-Ports editieren” auf Seite 51.

Anforderungen für VADP-Proxys auf vSnap-Servern

VADP-Proxys können in Ihrer IBM Spectrum Protect Plus-Umgebung auf vSnap-Servern installiert werden. Eine Kombination aus VADP-Proxy und vSnap-Server muss die Mindestanforderungen für beide Einheiten erfüllen. Ermitteln Sie mithilfe der Systemanforderungen für beide Einheiten, zu denen Sie die Kern- und RAM-Anforderungen addieren, die Mindestanforderungen für eine Kombination aus VADP-Proxy und vSnap-Server.

Stellen Sie sicher, dass Ihre Kombination aus VADP-Proxy und vSnap-Server die folgenden empfohlenen Mindestanforderungen, die die Summe der Anforderungen für jede Einheit sind, erfüllt.

VADP-Proxy-Installation auf einem virtuellen vSnap-Server:

- 64-Bit-Prozessor mit 8 Kernen
- 48 GB RAM

Alle erforderlichen VADP-Proxy- und vSnap-Server-Ports müssen für die Kombination aus VADP-Proxy und vSnap-Server offen sein. Die Abschnitte "VADP-Proxy-Ports" und "vSnap-Server-Ports" der Systemanforderungen enthalten weitere Informationen.

Cloudanforderungen

Wenn Daten in Cloudspeicher ausgelagert werden sollen, müssen Sie sicherstellen, dass Ihre IBM Spectrum Protect Plus- und Cloudumgebungen die folgenden Anforderungen erfüllen:

Plattencachebereich

Für die gesamte Funktionalität, die sich auf die Auslagerung in die Cloud oder die Zurückschreibung aus der Cloud bezieht, erfordert der vSnap-Server einen Plattencachebereich auf dem vSnap-Server.

- Während Auslagerungsoperationen wird dieser Cache als temporärer Staging-Bereich für Objekte verwendet, deren Upload in den Cloudendpunkt ansteht.
- Während Zurückschreibungsoperationen wird der Plattencachebereich zum Zwischenspeichern heruntergeladener Objekte sowie zum Speichern aller temporären Daten, die gegebenenfalls auf den Zurückschreibungsdatenträger geschrieben werden, verwendet.

Anweisungen zum Festlegen der Größe und zum Installieren des Cache finden Sie in Cloud offload configuration oder den IBM Spectrum Protect Plus Blueprints.

Zertifikatsanforderungen

- **Selbst signierte Zertifikate:** Wenn der Cloudendpunkt oder der Repository-Server ein selbst signiertes Zertifikat verwendet, muss das Zertifikat (im PEM-Format (PEM = Privacy Enhanced Mail)) angegeben werden, wenn der Cloud- oder Repository-Server in der IBM Spectrum Protect Plus-Benutzerschnittstelle registriert wird.
- **Von einer privaten Zertifizierungsstelle signierte Zertifikate:** Wenn der Cloudendpunkt oder der Repository-Server ein Zertifikat verwendet, das von einer privaten Zertifizierungsstelle (CA) signiert wurde, muss das Endpunktzertifikat (im PEM-Format) angegeben werden, wenn Sie den Cloud- oder Repository-Server in der IBM Spectrum Protect Plus-Benutzerschnittstelle registrieren. Außerdem muss das Stamm-/Zwischenzertifikat der privaten Zertifizierungsstelle (CA) dem Systemzertifikatsspeicher in jedem vSnap-Server mithilfe der folgenden Prozedur hinzugefügt werden:

  1. Melden Sie sich an der vSnap-Serverkonsole als Benutzer `serveradmin` an und laden Sie alle privaten CA-Zertifikate (im PEM-Format) in ein temporäres Verzeichnis hoch.
  2. Kopieren Sie jede Zertifikatsdatei in das Verzeichnis des Systemzertifikatsspeichers (`/etc/pki/ca trust/source/anchors/`), indem Sie den folgenden Befehl ausführen:

     ```
     $ sudo cp /tmp/private-ca-cert.pem /etc/pki/ca-trust/source/anchors/
     ```

3. Um das neu hinzugefügte angepasste Zertifikat einzufügen und das Systemzertifikatspaket zu aktualisieren, führen Sie den folgenden Befehl aus:

```
$ sudo update-ca-trust
```

- **Von einer öffentlichen Zertifizierungsstelle signierte Zertifikate:** Wenn der Cloudendpunkt ein öffentliches CA-signiertes Zertifikat verwendet, ist keine besondere Aktion erforderlich. Der vSnap-Server validiert das Zertifikat mithilfe des Standardsystemzertifikatsspeichers.

Netzanforderungen

Die folgenden Ports werden für die Kommunikation zwischen vSnap-Servern und Cloud- oder Repository-Server-Endpunkten verwendet.

Tabelle 7. Abgehende vSnap-Server-Firewallverbindungen

Port	Protokoll	Service	Beschreibung
443	TCP	HTTPS	Ermöglicht vSnap die Kommunikation mit Amazon S3-, Azure- oder IBM Cloud Object Storage-Endpunkten.
9000	TCP	HTTPS	Ermöglicht vSnap die Kommunikation mit IBM Spectrum Protect-(Repository-Server-)Endpunkten.

Alle Firewalls oder Netzproxys, die SSL Interception oder Deep Packet Inspection für den Datenverkehr zwischen vSnap-Servern und Cloudendpunkten ausführen, können die SSL-Zertifikatsvalidierung auf den vSnap-Servern beeinträchtigen. Diese Beeinträchtigung kann auch das Fehlschlagen von Cloudauslagerungsjobs zur Folge haben. Um diese Beeinträchtigung zu verhindern, müssen die vSnap-Server von SSL Interception und Deep Packet Inspection in der Firewall- oder Proxy-Konfiguration ausgeschlossen werden.

Cloud-Provider-Anforderungen

Die native Lebenszyklusverwaltung wird nicht unterstützt. IBM Spectrum Protect Plus verwaltet den Lebenszyklus hochgeladener Objekte automatisch mithilfe einer immer inkrementellen Lösung, bei der ältere Objekte weiterhin von neueren Momentaufnahmen verwendet werden können. Der automatische oder manuelle Verfall von Objekten außerhalb von IBM Spectrum Protect Plus hat fehlerhafte Daten zur Folge.

Wenn der Cloud-Provider ein selbst signiertes oder ein von einer privaten Zertifizierungsstelle signiertes SSL-Zertifikat verwendet, siehe Zertifikatsanforderungen.

Amazon S3-Cloudanforderungen

- **Auslagerung:** Wenn der Cloud-Provider in IBM Spectrum Protect Plus registriert wird, muss ein vorhandenes Bucket in einer der unterstützten Speichertiers angegeben werden: S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access, oder S3 One Zone-Infrequent Access.
- **Archivierung:** Wenn der Cloud-Provider in IBM Spectrum Protect Plus registriert wird, muss ein vorhandenes Bucket in einer der unterstützten Speichertiers angegeben werden: S3 Standard, S3 Intelligent-Tiering, S3 Standard-Infrequent Access oder S3 One Zone-Infrequent Access. IBM Spectrum Protect Plus lädt Datendateien direkt in das Glacier-Tier hoch. Einige kleine Metadatendateien werden im Standardtier für das Bucket gespeichert. Eine Kopie dieser Metadatendateien wird außerdem für die Wiederherstellung nach einem Katastrophenfall in das Glacier-Tier gestellt.

IBM Cloud Object Storage-Anforderungen

- **Auslagerung:** Wenn der Cloud-Provider in IBM Spectrum Protect Plus registriert wird, muss ein vorhandenes Bucket angegeben werden. Wenn die WORM-Richtlinie des angegebenen Buckets Objekte für eine bestimmte Zeit sperrt, erkennt IBM Spectrum Protect Plus automatisch die Konfiguration und löscht Momentaufnahmen, nachdem die Sperre von der WORM-Richtlinie entfernt wird.
- **Archivierung:** Wenn der Cloud-Provider in IBM Spectrum Protect Plus registriert wird, muss ein vorhandenes Bucket angegeben werden. Wenn die WORM-Richtlinie des angegebenen Buckets Objekte für eine bestimmte Zeit sperrt, erkennt IBM Spectrum Protect Plus automatisch die Konfiguration und löscht Momentaufnahmen, nachdem die Sperre von der WORM-Richtlinie entfernt wird. IBM Spectrum Protect Plus erstellt eine einzige Lebenszyklusverwaltungsregel in dem Bucket, um Datendateien in das Archivtier zu migrieren.

Microsoft Azure-Anforderungen

- **Auslagerung:** Wenn der Cloud-Provider in IBM Spectrum Protect Plus registriert wird, muss ein vorhandener Container in einem "heißen" oder "kalten" Speicheraccount angegeben werden.
- **Archivierung:** Wenn der Cloud-Provider in IBM Spectrum Protect Plus registriert wird, muss ein vorhandener Container in einem "heißen" oder "kalten" Speicheraccount angegeben werden. IBM Spectrum Protect Plus versetzt Dateien zwischen Tiers bedarfsgesteuert. Datendateien werden sofort in das Archivtier versetzt und nur während einer Zurückschreibungsoperation vorübergehend in das Tier für heiße Daten zurückversetzt. Einige kleine Metadatendateien werden im Standardtier für den Container gespeichert. Eine Kopie dieser Metadatendateien wird außerdem für die Wiederherstellung nach einem Katastrophenfall in das Archivtier gestellt.

IBM Spectrum Protect-(Repository-Server-)Anforderungen

- **Auslagerung:** Wenn der Cloud-Provider in IBM Spectrum Protect Plus registriert wird, können Sie kein vorhandenes Bucket verwenden. IBM Spectrum Protect Plus erstellt ein eindeutig benanntes Bucket für seine eigene Verwendung.
- **Archivierung:** Wenn der Cloud-Provider in IBM Spectrum Protect Plus registriert wird, können Sie kein vorhandenes Bucket verwenden. IBM Spectrum Protect Plus erstellt ein eindeutig benanntes Bucket für seine eigene Verwendung. IBM Spectrum Protect Plus lädt Datendateien direkt in IBM Spectrum Protect-Bandspeicher hoch. Einige kleine Metadatendateien werden im IBM Spectrum Protect-Objektspeicher gespeichert. Eine Kopie dieser Metadatendateien wird außerdem für die Wiederherstellung nach einem Katastrophenfall in IBM Spectrum Protect-Bandspeicher gestellt.

Tabelle 8. Auslagerungs- und Archivierungsanforderungen für Cloud-Provider

Operation	**Provider**	**Anforderungen**
Auslagerung	Amazon S3	Es muss ein vorhandenes Bucket in einem der unterstützten Speichertiers angegeben werden.
Auslagerung	IBM Cloud-Speicher	Es muss ein vorhandenes Bucket angegeben werden.
Auslagerung	Microsoft Azure	Es muss ein vorhandener Container im Speichertier für heiße oder kalte Daten angegeben werden.
Auslagerung	IBM Spectrum Protect	IBM Spectrum Protect Plus erstellt sein eigenes eindeutiges Bucket.

Tabelle 8. Auslagerungs- und Archivierungsanforderungen für Cloud-Provider (Forts.)		
Operation	**Provider**	**Anforderungen**
Archivierung	Amazon S3	Ermöglicht vSnap die Kommunikation mit IBM Spectrum Protect-(Repository-Server-)Endpunkten.
Archivierung	IBM Cloud-Speicher	Es muss ein vorhandenes Bucket im Archivtier angegeben werden.
Archivierung	Microsoft Azure	Es muss ein vorhandener Container im Speichertier für heiße Daten und im Archivtier angegeben werden.
Archivierung	IBM Spectrum Protect	IBM Spectrum Protect Plus erstellt sein eigenes eindeutiges Bucket, das in IBM Spectrum Protect-Bandspeicher kopiert wird.

Informationen für den Schnelleinstieg, die Sie beim Konfigurieren und Auslagern von Daten in bestimmte Cloud-Provider unterstützen, finden Sie in Data offload to cloud object storage with IBM Spectrum Protect Plus .

Hypervisoranforderungen

Überprüfen Sie die Hypervisoranforderungen für IBM Spectrum Protect Plus.

Um sicherzustellen, dass Sicherungs- und Zurückschreibungsoperationen erfolgreich ausgeführt werden können, muss Ihr System die Hardware- und Softwareanforderungen erfüllen. Die folgenden Anforderungen dienen als Ausgangspunkt. Die aktuellen Anforderungen, die unter Umständen Aktualisierungen umfassen, finden Sie in Technote 2013790.

Hyper-V-Anforderungen

Der Microsoft Hyper-V-Server muss die folgenden Mindestanforderungen erfüllen:

- Hyper-V Server 2016 oder Microsoft Hyper-V unter Windows Server 2016
- Microsoft Hyper-V unter Windows Server 2019

Die Sicherung und Zurückschreibung freigegebener virtueller Festplatten (freigegebene VHDX) wird nicht unterstützt. Informationen zu bekannten Problemen und Einschränkungen finden Sie in https://www.ibm.com/support/docview.wss?uid=ibm10884592.

IBM Spectrum Protect Plus schützt keine Umgebungen, in denen ein Hyper-V-Replikat aktiviert ist.

Der Microsoft-iSCSI-Initiator-Dienst muss auf allen Hyper-V-Servern, einschließlich Clusterknoten, aktiv sein. Legen Sie im Fenster **Dienste** als Starttyp für den Microsoft-iSCSI-Initiator-Dienst **Automatisch** fest, damit der Dienst beim Start des Hyper-V-Servers oder Clusterknotens verfügbar ist.

Der Parameter "automount" des Befehls **DiskPart** muss auf dem Hyper-V-Server aktiviert werden. Weitere Informationen zum Aktivieren des Parameters "automount" finden Sie unter dem Thema Automount auf der Microsoft-Website.

Hyper-V-Server können mithilfe eines DNS-Namens oder einer IP-Adresse registriert werden. DNS-Namen müssen von IBM Spectrum Protect Plus aufgelöst werden können. Wenn der Hyper-V-Server Teil eines Clusters ist, müssen alle Knoten in dem Cluster über DNS aufgelöst werden können. Wenn DNS nicht verfügbar ist, müssen Sie den Server der Datei `/etc/hosts` auf der IBM Spectrum Protect Plus-Appliance unter Verwendung der Befehlszeile hinzufügen. Wenn mehrere Hyper-V-Server in einer Clusterum-

gebung definiert sind, müssen Sie alle Server der Datei `/etc/hosts` hinzufügen. Wenn der Cluster in IBM Spectrum Protect Plus registriert wird, registrieren Sie den Failovercluster-Manager.

VMware-Anforderungen

Die folgenden VMware vSphere-Versionen werden unterstützt:

- vSphere 5.5, einschließlich aller Updates und Patch-Levels
- vSphere 6.0, einschließlich aller Updates und Patch-Levels
- vSphere 6.5, einschließlich aller Updates und Patch-Levels
- vSphere 6.7, einschließlich aller Updates und Patch-Levels

Stellen Sie sicher, dass die neueste Version von VMware Tools in Ihrer Umgebung installiert ist. IBM Spectrum Protect Plus wurde mit VMware Tools 9.10.0 getestet.

Physische RDM-Datenträger (pRDM-Datenträger) unterstützen keine Momentaufnahmen. Virtuelle Maschinen, die einen oder mehrere RDM-Datenträger enthalten, die im physischen Kompatibilitätsmodus (pRDM) bereitgestellt werden, werden gesichert. Die pRDM-Datenträger werden jedoch nicht im Rahmen der Sicherungsoperation für virtuelle Maschinen verarbeitet.

Dateiindexierungs- und -zurückschreibungsanforderungen

Überprüfen Sie die Dateiindexierungs- und -zurückschreibungsanforderungen für IBM Spectrum Protect Plus.

Um sicherzustellen, dass Sicherungs- und Zurückschreibungsoperationen erfolgreich ausgeführt werden können, muss Ihr System die Hardware- und Softwareanforderungen erfüllen. Die folgenden Anforderungen dienen als Ausgangspunkt. Die aktuellen Anforderungen, die unter Umständen Aktualisierungen umfassen, finden Sie in Technote 2013790.

iSCSI-Platten, die direkt dem Gastbetriebssystem zugeordnet werden, werden nicht indexiert. Unterstützte Datenträger umfassen VMDK- oder VHD-Datenträger, die über die Konfiguration der zugeordneten virtuellen Maschine bereitgestellt werden.

Wie viel freier Speicherbereich für die Metadaten in dem Katalog erforderlich ist, ist von der Gesamtzahl Dateien abhängig, die in der Umgebung vorhanden sind. Um 1 Million Dateien zu katalogisieren, ist für den Katalogdatenträger in der IBM Spectrum Protect Plus-Appliance etwa 350 MB freier Speicherbereich pro aufbewahrter Version erforderlich. Der von Dateiindexierungsmetadaten belegte Speicherbereich wird konsolidiert, wenn die entsprechenden Sicherungsinstanzen verfallen.

VMware-Anforderungen

In den Einstellungen für die virtuelle Maschine muss bei der erweiterten Konfiguration die Einstellung disk.enableUUID vorhanden und auf true gesetzt sein.

Windows-Anforderungen

Unterstützte Betriebssysteme	• Windows Server 2008 R2 • Windows Server 2012 R2 und Windows Server 2012 R2 Core • Windows Server 2016 und Windows Server 2016 Core • Windows Server 2019 und Windows Server 2019 Core
Unterstützte Dateisysteme	• NTFS • ReFS • CsvFS

Unterstützte Plattenspeichertypen	Basisplatten mit • MBR-Partitionen • GPT-Partitionen **Einschränkung:** Die Sicherung oder Zurückschreibung von Dateien auf dynamischen Platten wird nicht unterstützt.

- IBM Spectrum Protect Plus unterstützt nur die Betriebssysteme, die für Ihre Hypervisoren verfügbar sind. Überprüfen Sie die Dokumentation Ihres Hypervisors auf Informationen zu unterstützten Betriebssystemen.
- Dateiindexierungs- und -zurückschreibungsoperationen unterstützen SCSI-Platten in einer Hyper-V-Umgebung. IDE-Platten (IDE = Integrated Drive Electronics) werden nicht unterstützt. Beachten Sie, dass virtuelle Maschinen der Generation 1 IDE-Bootplatten erfordern; wenn jedoch zusätzliche SCSI-Platten verfügbar sind, werden Dateiindexierungs- und -zurückschreibungsoperationen auf diesen Platten unterstützt.
- Windows Remote Shell (WinRM) muss aktiviert sein.

  Wichtig: IBM Spectrum Protect Plus kann virtuelle Maschinen mit anderen Dateisystemen schützen und zurückschreiben, für die Dateiindexierung und -zurückschreibung sind jedoch nur die zuvor aufgelisteten Dateisysteme auswählbar.
- Wenn die Dateiindexierung in einer Windows-Umgebung ausgeführt wird, werden die folgenden Verzeichnisse in der Ressource übersprungen:

  ```
  \Drivers
  \Programme
  \Programme (x86)
  \Windows
  \winnt
  ```

  Anmerkung: Dateien in diesen Verzeichnissen werden nicht dem IBM Spectrum Protect Plus-Bestand hinzugefügt und sind für die Dateiwiederherstellung nicht verfügbar.
- Stellen Sie sicher, dass die neueste Version von VMware Tools auf den virtuellen VMware-Maschinen installiert ist und Hyper-V Integration Services auf Ihren virtuellen Hyper-V-Maschinen installiert ist.

Speicheranforderungen

- Auf dem Laufwerk `C:\` muss genügend temporärer Speicherbereich vorhanden sein, um die Ergebnisse der Dateiindexierung speichern zu können.
- Wenn Dateisysteme indexiert werden, werden temporäre Metadatendateien unter dem Verzeichnis `/tmp` erstellt und anschließend gelöscht, sobald die Indexierung abgeschlossen ist. Wie viel freier Speicherbereich für die Metadaten erforderlich ist, ist von der Gesamtzahl Dateien abhängig, die auf dem System vorhanden sind. Stellen Sie sicher, dass pro 1 Million Dateien etwa 350 MB freier Speicherbereich vorhanden ist.

Konnektivitätsanforderungen

- Der Hostname der IBM Spectrum Protect Plus-Appliance muss von der virtuellen Windows-Maschine auflösbar sein.
- Die IP-Adresse der für die Indexierung ausgewählten virtuellen Maschine muss für den vSphere-Client oder Hyper-V-Manager sichtbar sein.
- Die für die Indexierung ausgewählte virtuelle Windows-Maschine muss abgehende Verbindungen zu Port 22 (SSH) auf der IBM Spectrum Protect Plus-Appliance ermöglichen.
- Alle Firewalls müssen so konfiguriert sein, dass sie IBM Spectrum Protect Plus das Herstellen der Verbindung zum Server mithilfe von WinRM ermöglichen.

Authentifizierungs- und Berechtigungsanforderungen

Die für die virtuelle Maschine angegebenen Berechtigungsnachweise müssen einen Benutzer mit den folgenden Berechtigungen umfassen:

- Der Benutzeridentität muss das Recht "Anmelden als Dienst" zugeordnet sein; diese Zuordnung erfolgt über "Verwaltung" unter "Systemsteuerung" auf der lokalen Maschine (**Lokale Sicherheitsrichtlinie** > **Lokale Richtlinien** > **Zuweisen von Benutzerrechten** > **Anmelden als Dienst**).

  Weitere Informationen zur Berechtigung "Anmelden als Dienst" finden Sie in Add the Log on as a service Right to an Account.
- Die Standardsicherheitsrichtlinie verwendet das Windows-NTLM-Protokoll und die Benutzeridentität folgt dem Standardformat `Domäne\Name`, wenn die virtuelle Hyper-V-Maschine einer Domäne zugeordnet ist. Das Format `<lokaler Administrator>` wird verwendet, wenn der Benutzer ein lokaler Administrator ist. Beachten Sie, dass Berechtigungsnachweise für die zugeordnete virtuelle Maschine mithilfe der Optionen **Benutzername für Gastbetriebssystem** und **Kennwort für Gastbetriebssystem** in der zugehörigen Sicherungsjobdefinition erstellt werden müssen.
- Der Systemanmeldeberechtigungsnachweis muss über die Berechtigungen des lokalen Administrators verfügen.

Kerberos-Anforderungen

- Die Kerberos-basierte Authentifizierung kann über eine Konfigurationsdatei in der IBM Spectrum Protect Plus-Appliance aktiviert werden. Mit dieser Einstellung wird das standardmäßige Windows-NTLM-Protokoll außer Kraft gesetzt. Beachten Sie, dass Kerberos nicht die Verwendung lokaler Benutzeraccounts ermöglicht und nur für Umgebungen geeignet ist, in denen sich alle Maschinen in einer einzigen Domäne befinden.
- Nur für die Kerberos-basierte Authentifizierung muss die Benutzeridentität im Format `Benutzername@FQDN` angegeben werden. Der angegebene Benutzer muss sich mit dem registrierten Kennwort authentifizieren können, um ein Ticket-Granting-Ticket (TGT) vom Key-Distribution-Center (KDC) in der Domäne anzufordern, die mit dem vollständig qualifizierten Domänennamen (FQDN) angegeben wird.
- Für die Kerberos-Authentifizierung muss außerdem die Zeitabweichung zwischen dem Domänencontroller und der IBM Spectrum Protect Plus-Appliance weniger als 5 Minuten betragen. Beachten Sie, dass das standardmäßige Windows-NTLM-Protokoll nicht zeitabhängig ist.

Linux-Anforderungen

Unterstützte Betriebssysteme	• Red Hat Enterprise Linux 6.4 und höhere Wartungs- und Modifikationsstufen • CentOS 6.4 und höhere Wartungs- und Modifikationsstufen • Red Hat Enterprise Linux 7.0 und höhere Wartungs- und Modifikationsstufen • CentOS 7.0 und höhere Wartungs- und Modifikationsstufen • SUSE Linux Enterprise Server 12.0 und höhere Wartungs- und Modifikationsstufen
Unterstützte Dateisysteme	• ext2 • ext3 • ext4 • XFS

- Ein Dateisystem, das unter einer neueren Kernelversion erstellt wurde, kann möglicherweise nicht auf einem System mit einem älteren Kernel bereitgestellt werden; in diesem Fall wird die Zurückschreibung von Dateien von dem neueren System in das ältere System nicht unterstützt.

  IBM Spectrum Protect Plus unterstützt nur die Betriebssysteme, die für Ihre Hypervisoren verfügbar sind. Überprüfen Sie die Dokumentation Ihres Hypervisors auf Informationen zu unterstützten Betriebssystemen.

  Anmerkung: IBM Spectrum Protect Plus kann virtuelle Maschinen mit anderen Dateisystemen schützen und zurückschreiben, für die Dateiindexierung und -zurückschreibung sind jedoch nur die zuvor aufgelisteten Dateisysteme auswählbar.
- Wenn die Dateiindexierung in einer Linux-Umgebung ausgeführt wird, werden die folgenden Verzeichnisse in der Ressource übersprungen:

  ```
  /tmp
  /usr/bin
  /Drivers
  /bin
  /sbin
  ```
- Dateien in virtuellen Dateisystemen wie `/proc`, `/sys` und `/dev` werden ebenfalls übersprungen. Dateien in diesen Verzeichnissen werden nicht dem IBM Spectrum Protect Plus-Bestand hinzugefügt und sind für die Dateiwiederherstellung nicht verfügbar.

Speicheranforderungen

- Die Systemplatte muss über genügend temporären Speicherbereich verfügen, um die Ergebnisse der Dateiindexierung speichern zu können.
- Wenn Dateisysteme indexiert werden, werden temporäre Metadatendateien unter dem Verzeichnis `/tmp` erstellt und anschließend gelöscht, sobald die Indexierung abgeschlossen ist. Wie viel freier Speicherbereich für die Metadaten erforderlich ist, ist von der Gesamtzahl Dateien abhängig, die auf dem System vorhanden sind. Stellen Sie sicher, dass pro 1 Million Dateien etwa 350 MB freier Speicherbereich vorhanden ist.

Softwareanforderungen

- Python Version 2.6 (beliebiger Stand) oder 2.7 (beliebiger Stand) muss installiert sein.
- Nur Red Hat Enterprise Linux/CentOS 6.x: Stellen Sie sicher, dass das Paket `util-linux-ng` aktuell ist, indem Sie **`yum update util-linux-ng`** ausführen. Abhängig von Ihrer Version oder Distribution kann das Paket den Namen `util-linux` haben.
- Wenn Daten auf LVM-Datenträgern gespeichert sind, stellen Sie sicher, dass die LVM-Version 2.0.2.118 oder höher ist. Führen Sie **`lvm version`** aus, um die Version zu überprüfen; führen Sie, falls erforderlich, **`yum update lvm2`** aus, um das Paket zu aktualisieren.
- Wenn sich Daten auf LVM-Datenträgern befinden, muss der Service **`lvm2-lvmetad`** inaktiviert werden, da er die Fähigkeit von IBM Spectrum Protect Plus, Momentaufnahmen oder Klone der Datenträgergruppe bereitzustellen und erneut zu signieren, beeinträchtigen kann. Führen Sie die folgenden Schritte aus, um den Service zu inaktivieren:

  1. Führen Sie die folgenden Befehle aus:

     ```
     systemctl stop lvm2-lvmetadsystemctl disable lvm2-lvmetad
     ```
  2. Editieren Sie `/etc/lvm/lvm.conf` und geben Sie die folgende Einstellung an:

     ```
     use_lvmetad = 0
     ```

     Ausführliche Informationen zum Service **`lvmetad`** finden Sie in The Metadata Daemon (lvmetad).
- Wenn sich Daten auf XFS-Dateisystemen befinden und die Version von **`xfsprogs`** zwischen 3.2.0 und 4.1.9 liegt, kann die Dateizurückschreibung aufgrund eines bekannten Problems in **`xfsprogs`**, das die Beschädigung eines Klon- oder Momentaufnahmedateisystems zur Folge hat, wenn seine

UUID geändert wird, fehlschlagen. Aktualisieren Sie zur Lösung dieses Problems **xfsprogs** mit Version 4.2.0 oder höher.

Weitere Informationen finden Sie in Debian Bug report logs.

Konnektivitätsanforderungen

Der SSH-Service muss an Port 22 auf dem Server aktiv sein und alle Firewalls müssen so konfiguriert sein, dass sie IBM Spectrum Protect Plus das Herstellen der Verbindung zum Server mit SSH ermöglichen. Das Subsystem SFTP für SSH muss ebenfalls aktiviert sein.

Authentifizierungs- und Berechtigungsanforderungen

Die für die virtuelle Maschine angegebenen Berechtigungsnachweise müssen einen Benutzer mit den folgenden **sudo**-Berechtigungen angeben:

- Die `sudoers`-Konfiguration muss dem Benutzer die Ausführung von Befehlen ohne Kennwort ermöglichen.
- Die Einstellung !requiretty muss definiert sein.

Es wird empfohlen, einen dedizierten IBM Spectrum Protect Plus-Agentenbenutzer mit den folgenden Berechtigungen zu erstellen. Beispielkonfiguration:

- Erstellen Sie einen Benutzer: `useradd -m sppagent`

  Dabei gibt **sppagent** den IBM Spectrum Protect Plus-Agentenbenutzer an.
- Legen Sie ein Kennwort fest: `passwd <sppagent>`

Fügen Sie am Ende Ihrer `sudoers`-Konfigurationsdatei (in der Regel `/etc/sudoers`) die folgenden Zeilen hinzu. Wenn Ihre vorhandene `sudoers`-Datei für den Import von Konfigurationen aus einem anderen Verzeichnis (beispielsweise `/etc/sudoers.d`) konfiguriert ist, können Sie die Zeilen auch in eine neue Datei in diesem Verzeichnis stellen:

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

Microsoft Exchange Server-Anforderungen

Informieren Sie sich vor der Installation von IBM Spectrum Protect Plus über die Hardware- und Softwareanforderungen für die Produktkomponenten und anderen Komponenten.

Um sicherzustellen, dass Sicherungs- und Zurückschreibungsoperationen erfolgreich ausgeführt werden können, muss Ihr System die Hardware- und Softwareanforderungen erfüllen. Die folgenden Anforderungen dienen als Ausgangspunkt. Die aktuellen Anforderungen, die unter Umständen Aktualisierungen umfassen, finden Sie in Technote 2013790.

Die Exchange-Datenbanksicherungs- und -zurückschreibungsanforderungen für IBM Spectrum Protect Plus sind wie folgt.

Konfiguration

Stellen Sie sicher, dass die von Ihnen verwendete Microsoft Exchange Server-Version unter Ihrem Betriebssystem unterstützt wird.

Anwendungsversionen

- Microsoft Exchange Server 2013 CU16 und höhere CU- und Wartungsstufen: Standard Edition oder Enterprise Edition
- Microsoft Exchange Server 2016 CU5 und höhere CU- und Wartungsstufen: Standard Edition und Enterprise Edition
- Microsoft Exchange Server 2019 und höhere Wartungsstufen: Standard Edition und Enterprise Edition

Anmerkung: Microsoft Exchange-Datenbankverfügbarkeitsgruppen (DAG) werden unterstützt.

Betriebssysteme

- Windows Server 2012R2 und höhere Wartungsstufen (64-Bit-Kernel): Standard Edition und Datacenter Edition
- Windows Server 2016 und höhere Wartungsstufen (64-Bit-Kernel): Standard Edition und Datacenter Edition
- Windows Server 2019 und höhere Wartungsstufen (64-Bit-Kernel): Standard Edition und Datacenter Edition

Anmerkung: Die Windows Server 2019 Core-Installation wird unterstützt. Die Funktion für differenzierte Zurückschreibung wird in einer Core-Installation jedoch nicht unterstützt.

Weitere Hinweise

Installieren Sie die neuesten Microsoft Exchange Server-Patchs und -aktualisierungen in Ihrer Umgebung.

Informationen zur Virtualisierungsunterstützung für Exchange Server finden Sie in „Voraussetzungen für Microsoft Exchange Server" auf Seite 168.

Software

Stellen Sie sicher, dass eine unterstützte Version eines Windows-64-Bit-Betriebssystems installiert ist.

Die folgenden Microsoft-Voraussetzungen sind erforderlich und müssen installiert werden, bevor IBM Spectrum Protect Plus verwendet wird:

- Windows PowerShell 4 oder höher
- Windows Management Framework 4 oder höher

Wenn Microsoft Exchange Server 2013 und die Funktion für differenzierte Zurückschreibung verwendet werden, ist die für Microsoft Exchange Messaging API (MAPI) Client and Collaboration Data Objects (MAPI/CDO) unterstützte Mindestversion 6.5.8320.0.

Anmerkung: MAPI/CDO ist nur für Microsoft Exchange Server 2013 erforderlich. Es ist nicht erforderlich, wenn Sie Microsoft Exchange Server 2016 oder Exchange Server 2019 ausführen.

Wenn Sie die Funktion für differenzierte Zurückschreibung mit Microsoft Exchange Server 2016 oder Microsoft Exchange Server 2019 verwenden, ist die 32-Bit-Version von Microsoft Outlook 2016 oder die 32-Bit-Version von Microsoft Outlook 2019 erforderlich.

Die folgenden Microsoft-Voraussetzungen sind erforderlich und werden automatisch von der IBM Spectrum Protect Plus-Funktion für differenzierte Zurückschreibung installiert, wenn sie nicht bereits auf Ihrer virtuellen Maschine vorhanden sind.

- Microsoft Visual C++ 2012 Redistributable Package (32-Bit-Version)
- Microsoft Visual C++ 2012 Redistributable Package (64-Bit-Version)
- Microsoft Visual C++ 2017 Redistributable Package (32-Bit-Version)
- Microsoft Visual C++ 2017 Redistributable Package (64-Bit-Version)
- Microsoft .NET Framework 4.5
- Microsoft ReportViewer 2012 SP1 Redistributable
- Microsoft SQL Server 2012-System-CLR-Typen
- Microsoft SQL Server 2014-System-CLR-Typen
- Microsoft SQL Server 2016-System-CLR-Typen

Tipp: Die Installation dieser Voraussetzungen kann unter Umständen einen Systemneustart erfordern. Um einen Systemneustart zu verhindern, stellen Sie sicher, dass diese Voraussetzungen installiert sind, bevor Sie die IBM Spectrum Protect Plus-Funktion für differenzierte Zurückschreibung starten.

Berechtigungen

IBM Spectrum Protect Plus-Agentenbenutzer müssen über die folgenden Berechtigungen verfügen:

Microsoft Exchange Server wird durch die rollenbasierte Authentifizierung geschützt. Damit der Microsoft Exchange-Agent in Ihrer IBM Spectrum Protect Plus-Umgebung funktionsfähig ist, müssen Sie die entsprechenden Berechtigungen festlegen. Weitere Informationen finden Sie in „Berechtigungen” auf Seite 168.

Ports

Die folgenden Ports werden von IBM Spectrum Protect Plus-Agentenbenutzern verwendet. Ports, die in der Spalte "Firewallregel" mit "Accept" angegeben sind, verwenden sichere Verbindungen (HTTPS oder SSL).

Tabelle 9. Eingehende IBM Spectrum Protect Plus-Agentenfirewallverbindungen

Port	Protokoll	Firewallregel	Service	Beschreibung
5985	TCP	Accept	WinRM	Windows-Remoteverwaltungsdienst
5986	TCP	Accept	WinRM	Sicherer Windows-Remoteverwaltungsdienst

Tabelle 10. Abgehende IBM Spectrum Protect Plus-Agentenfirewallverbindungen

Port	Protokoll	Service	Beschreibung
3260*	TCP	vSnap-iSCSI	iSCSI-vSnap-Zielport, der zur Bereitstellung von LUNs für die Sicherung und Wiederherstellung verwendet wird
137	UDP	vSnap-SMB/-CIFS	vSnap-SMB- oder -CIFS-Zielport, der zur Bereitstellung von Dateisystemfreigaben für die Transaktionsprotokollsicherung und -wiederherstellung verwendet wird
138	UDP	vSnap-SMB/-CIFS	vSnap-SMB- oder -CIFS-Zielport, der zur Bereitstellung von Dateisystemfreigaben für die Transaktionsprotokollsicherung und -wiederherstellung verwendet wird
139	TCP	vSnap-SMB/-CIFS	vSnap-SMB- oder -CIFS-Zielport, der zur Bereitstellung von Dateisystemfreigaben für die Transaktionsprotokollsicherung und -wiederherstellung verwendet wird

Tabelle 10. Abgehende IBM Spectrum Protect Plus-Agentenfirewallverbindungen (Forts.)			
Port	**Protokoll**	**Service**	**Beschreibung**
445	TCP	vSnap-SMB/-CIFS	vSnap-SMB- oder -CIFS-Zielport, der zur Bereitstellung von Dateisystemfreigaben für die Transaktionsprotokollsicherung und -wiederherstellung verwendet wird

*Auf diesem Knoten ist der iSCSI-Initiator erforderlich.

Hardware

System	**Plattenspeicher**	**Plattenspeicher für Operationen für differenzierte Zurückschreibung**
x64: Kompatible Hardware, die vom Betriebssystem und von Microsoft Exchange Server unterstützt wird	Mindestens 200 MB Plattenspeicher für das Produkt, das installiert werden soll	Mindestens 2,1 GB Plattenspeicher für "Zusätzliche Microsoft-Voraussetzungen", die automatisch installiert werden, sofern noch nicht bereits installiert

Db2-Anforderungen

Stellen Sie vor der Registrierung von Db2 bei IBM Spectrum Protect Plus sicher, dass Ihre Umgebung die angegebenen Anforderungen erfüllt.

Um sicherzustellen, dass Sicherungs- und Zurückschreibungsoperationen erfolgreich ausgeführt werden können, muss Ihr System die Hardware- und Softwareanforderungen erfüllen. Die folgenden Anforderungen dienen als Ausgangspunkt. Die aktuellen Anforderungen, die unter Umständen Aktualisierungen umfassen, finden Sie in Technote 2013790.

Die IBM Db2-Datenbanksicherungs- und -zurückschreibungsanforderungen für IBM Spectrum Protect Plus sind wie folgt.

Konfigurationsanforderungen

Die folgenden IBM Db2-Datenbanken werden unterstützt:

- IBM Db2 Version 10.5 und höhere Wartungsstufen und Modifikationsstufen: Enterprise Server Edition
- IBM Db2 Version 11.1 und höhere Wartungsstufen und Modifikationsstufen: Enterprise Server Edition

Betriebssysteme

Die folgenden Betriebssysteme werden unterstützt:

- Unter PowerPC:
  - AIX 7.1 und höhere Modifikations- und Fixpackstufen (64-Bit-Kernel)
  - AIX 7.2 und höhere Modifikations- und Fixpackstufen (64-Bit-Kernel)
- Unter Linux x86_x64:
  - Red Hat Enterprise Linux 6.8 und höhere Wartungsstufen und Modifikationsstufen
  - Red Hat Enterprise Linux 7 und höhere Wartungsstufen und Modifikationsstufen
  - SUSE Linux Enterprise Server 11.0 SP4 und höhere Wartungsstufen und Modifikationsstufen

  - SUSE Linux Enterprise Server 12.0 SP1 und höhere Wartungsstufen und Modifikationsstufen
- Unter Linux on Power Systems (Little Endian)
  - Red Hat Enterprise Linux 7.1 und höhere Wartungs- und Modifikationsstufen
  - SUSE Linux Enterprise Server 12.0 SP1 und höhere Wartungs- und Modifikationsstufen

Weitere Hinweise

Installieren Sie die neuesten IBM Db2-Patchs und -Aktualisierungen in Ihrer Umgebung.

IBM Db2 pureScale wird nicht unterstützt.

Stellen Sie sicher, dass Ihre Db2-Umgebung so konfiguriert ist, dass sie die folgenden Kriterien erfüllt:

- Die Db2-Archivprotokollierung ist aktiviert und Db2 befindet sich in einem wiederherstellbaren Modus.
- Logische Datenträger, die Db2-Tabellenbereiche (Daten und Tabellenbereiche für temporäre Tabellen), das lokale Datenbankverzeichnis und Db2-Protokolldateien enthalten, werden unter Linux von Logical Volume Manager (LVM2) bzw. unter AIX von JFS2 verwaltet. LVM2 unter Linux und JFS2 unter AIX werden zum Erstellen temporärer Datenträgermomentaufnahmen verwendet. Die Größe des logischen Datenträgers nimmt in dem Maße zu, wie sich Daten auf dem Quellendatenträger während der Lebensdauer der Momentaufnahme ändern. Weitere Informationen finden Sie in „LVM2 und JFS2" auf Seite 146.
- Db2 muss sich im Modus für parallele Sicherung befinden, wenn mehrere Partitionen geschützt werden sollen. Der Modus für parallele Sicherung kann mithilfe von Db2-Registry-Variablen aktiviert werden. Weitere Informationen finden Sie in „Voraussetzungen für Db2" auf Seite 143.

Software

Überprüfen Sie die folgenden Softwareanforderungen:

- Die bash- und sudo-Pakete müssen installiert sein. Sudo muss Version 1.7.6p2 oder höher haben. Führen Sie sudo -V aus, um die Version zu überprüfen.

  Anmerkung: Die erforderlichen bash- und sudo-Pakete sind in die unterstützten Linux 86_64- und Linux Power Systems (Little Endian)-Betriebssysteme eingeschlossen.
- Python Version 2.6 (beliebiger Stand) oder 2.7 (beliebiger Stand) muss unter Linux installiert sein.
- Python Version 2.7.x muss unter AIX installiert sein.
- Stellen Sie sicher, dass die unterstützte Version von Linux x86_64, Linux Power Systems (Little Endian) oder AIX installiert ist.

Konnektivität

Stellen Sie sicher, dass die folgenden Konnektivitätskriterien erfüllt sind:

- Der SSH-Service ist an Port 22 auf dem Server aktiv.
- Firewalls müssen so konfiguriert sein, dass sie IBM Spectrum Protect Plus das Herstellen der Verbindung zum Server mithilfe von SSH ermöglichen.
- Das Subsystem SFTP für SSH ist aktiviert.
- Der Server kann mithilfe eines DNS-Namens oder einer IP-Adresse registriert werden. DNS-Namen müssen von IBM Spectrum Protect Plus aufgelöst werden können.
- Stellen Sie unter AIX sicher, dass die NFS-Kommunikation mit reservierten Ports konfiguriert ist, indem Sie den folgenden Befehl verwenden: **`nfso -p -o nfs_use_reserved_port=1`**

Authentifizierung und Berechtigungen

Der Db2-Server muss in IBM Spectrum Protect Plus unter Verwendung eines Betriebssystembenutzers, der auf dem Db2-Server vorhanden ist (er wird als IBM Spectrum Protect Plus-Agentenbenutzer bezeichnet), registriert werden.

Stellen Sie sicher, dass das Kennwort korrekt konfiguriert ist und sich der Benutzer anmelden kann, ohne dass weitere Eingabeaufforderungen, wie beispielsweise Eingabeaufforderungen zum Zurücksetzen des Kennworts, angezeigt werden.

Der IBM Spectrum Protect Plus-Agentenbenutzer muss über die folgenden Berechtigungen verfügen:

- Berechtigungen zur Ausführung von Befehlen als Rootbenutzer und als Db2-Softwareeigner unter Verwendung von sudo. Dies ist für IBM Spectrum Protect Plus erforderlich, um verschiedene Tasks, wie beispielsweise das Erkennen von Speicherlayouts, das Bereitstellen von Platten und das Aufheben der Bereitstellung von Platten sowie das Verwalten von Datenbanken, ausführen zu können.
  - Die sudoers-Konfiguration muss dem IBM Spectrum Protect Plus-Agentenbenutzer die Ausführung von Befehlen ohne Kennwort ermöglichen.
  - Die Einstellung `!requiretty` muss definiert sein.
- Berechtigungen zum Lesen des Db2-Bestands mithilfe von `/usr/local/bin/db2ls`. Diese Berechtigungen sind für IBM Spectrum Protect Plus erforderlich, um Informationen zu IBM Db2-Instanzen und -Datenbanken erkennen und erfassen zu können.

Ports

Die folgenden Ports werden von IBM Spectrum Protect Plus-Agenten verwendet. Ports, die mit "Accept" gekennzeichnet sind, verwenden eine sichere Verbindung (HTTPS/SSL).

Tabelle 11. Eingehende IBM Spectrum Protect Plus-Agentenfirewallverbindungen

Port	Protokoll	Firewall	Service	Beschreibung
22	TCP	Accept	SSH	Für die SSH-Datenübertragung zum und vom internen vSnap-Server verwendet.

Tabelle 12. Abgehende IBM Spectrum Protect Plus-Agentenfirewallverbindungen

Port	Protokoll	Service	Beschreibung
111	TCP	vSnap RPC Port Bind	Ermöglicht Clients das Erkennen von Ports, die ONC-Clients (ONC = Open Network Computing) für die Kommunikation mit ONC-Servern erfordern
2049	TCP	vSnap NFS	Für die NFS-Dateifreigabe über vSnap verwendet.
20048	TCP	vSnap NFS Mount	Stellt vSnap-Dateisysteme auf Clients, wie beispielsweise dem VADP-Proxy, Anwendungsservern und Virtualisierungsdatenspeichern, bereit.

MongoDB-Anforderungen

Stellen Sie vor der Registrierung von MongoDB bei IBM Spectrum Protect Plus sicher, dass Ihre Umgebung die angegebenen Anforderungen erfüllt.

Um sicherzustellen, dass Sicherungs- und Zurückschreibungsoperationen erfolgreich ausgeführt werden können, muss Ihr System die Hardware- und Softwareanforderungen erfüllen. Die folgenden Anforderungen dienen als Ausgangspunkt. Die aktuellen Anforderungen, die unter Umständen Aktualisierungen umfassen, finden Sie in Technote 2013790.

Die MongoDB-Datenbanksicherungs- und -zurückschreibungsanforderungen für IBM Spectrum Protect Plus sind wie folgt.

Konfigurationsanforderungen

Die folgenden MongoDB-Datenbankversionen werden unterstützt:

- MongoDB Version 3.6 und höhere Wartungsstufen und Modifikationsstufen: Community Server Edition und Enterprise Server Edition
- MongoDB Version 4.0 und höhere Wartungsstufen und Modifikationsstufen: Community Server Edition und Enterprise Server Edition

Betriebssysteme

Die folgenden Betriebssysteme werden unterstützt:

- Unter Linux x86_x64:
  - Red Hat Enterprise Linux 6.8 und höhere Wartungsstufen und Modifikationsstufen
  - CentOS 6.8 und höhere Wartungsstufen und Modifikationsstufen
  - Red Hat Enterprise Linux 7 und höhere Wartungsstufen und Modifikationsstufen
  - CentOS 7 und höhere Wartungsstufen und Modifikationsstufen
  - SUSE Linux Enterprise Server 12.0 SP1 und höhere Wartungsstufen und Modifikationsstufen
- Unter Linux Power Systems (Little Endian)
  - Red Hat Enterprise Linux 7.1 und höhere Wartungs- und Modifikationsstufen
  - CentOS 7 und höhere höhere Wartungs- und Modifikationsstufen

Hinweis: Unter Linux Power Systems (Little Endian) wird nur MongoDB Enterprise Server Edition unterstützt.

Weitere Hinweise

Installieren Sie zur Leistungsoptimierung die neuesten MongoDB-Patchs und -Aktualisierungen, die für Ihre Umgebung verfügbar sind.

Stellen Sie sicher, dass Ihre MongoDB-Umgebung so konfiguriert ist, dass sie die folgenden Kriterien erfüllt:

- MongoDB ist als eigenständige Instanz oder als Replikatgruppe konfiguriert. Sicherungsoperationen von sharded MongoDB-Clusterinstanzen werden nicht unterstützt. Eine Sicherung umfasst immer alle Datenbanken in der Instanz.
- Die MongoDB-Instanz ist für die Verwendung der WiredTiger-Speicherengine konfiguriert.
- Der Benutzer in der MongoDB-Anwendungsserverregistrierung in IBM Spectrum Protect Plus muss Serverinformationen und den Status aus der MongoDB-Administratordatenbank abrufen können.
- Logische Datenträger von MongoDB-Daten und Protokollpfade werden von Linux Logical Volume Manager (LVM2) verwaltet. LVM2 wird zum Erstellen temporärer Datenträgermomentaufnahmen verwendet. Die Datenbankdateien und das Journal müssen sich auf einem einzigen Datenträger befinden. Die Größe des logischen Datenträgers nimmt in dem Maße zu, wie sich Daten auf dem Quellendatenträger wäh-

rend der Lebensdauer der Momentaufnahme ändern. Weitere Informationen finden Sie in „Linux-LVM2" auf Seite 207.

Software

Überprüfen Sie die folgenden Softwareanforderungen:

- Die Python-Version Version 2.6 (beliebiger Stand) oder Version 2.7 (beliebiger Stand) muss installiert sein.
- Wenn der MongoDB-Anwendungsserver RHEL 6 oder CentOS 6, ausführt, stellen Sie sicher, dass das `openssl`-Paket Version 1.0.1e-57 oder höher hat. Führen Sie `"yum update openssl"` aus, um diese Anforderung zu aktualisieren.
- Stellen Sie sicher, dass die unterstützte Version von Linux x86_64 oder Linux Power Little Endian installiert ist.

Konnektivität

Stellen Sie sicher, dass die folgenden Konnektivitätskriterien erfüllt sind:

- Der SSH-Service ist an Port 22 auf dem Server aktiv.
- Firewalls müssen so konfiguriert sein, dass sie IBM Spectrum Protect Plus das Herstellen der Verbindung zum Server mithilfe von SSH ermöglichen.
- Das Subsystem SFTP für SSH ist aktiviert.
- Der Anwendungsserver kann in IBM Spectrum Protect Plus mithilfe eines DNS-Namens oder einer IP-Adresse registriert werden. DNS-Namen müssen von IBM Spectrum Protect Plus aufgelöst werden können.

Authentifizierung und Berechtigungen

Der MongoDB-Server muss in IBM Spectrum Protect Plus unter Verwendung eines Betriebssystembenutzers, der auf dem MongoDB-Server vorhanden ist (er wird im restlichen Teil dieses Abschnitts als *IBM Spectrum Protect Plus-Agentenbenutzer* bezeichnet), registriert werden.

Stellen Sie sicher, dass das Kennwort korrekt konfiguriert ist und sich der Benutzer anmelden kann, ohne dass weitere Eingabeaufforderungen, wie beispielsweise Eingabeaufforderungen zum Zurücksetzen des Kennworts, angezeigt werden.

Unter MongoDB werden die SSL-basierte Verschlüsselung und zertifikatbasierte Authentifizierung nicht unterstützt.

Unter MongoDB Enterprise Server Editions wird nur die Speicherverschlüsselung unterstützt.

Der IBM Spectrum Protect Plus-Agentenbenutzer muss über die folgenden Berechtigungen verfügen:

- Berechtigungen zur Ausführung von Befehlen als Rootbenutzer und als MongoDB-Softwareeigner unter Verwendung von sudo. Diese Berechtigung ist für IBM Spectrum Protect Plus erforderlich, um Tasks, wie beispielsweise das Erkennen von Speicherlayouts, das Bereitstellen von Platten und das Aufheben der Bereitstellung von Platten sowie das Verwalten von Datenbanken, ausführen zu können.
  - Die sudoers-Konfiguration muss dem IBM Spectrum Protect Plus-Agentenbenutzer die Ausführung von Befehlen ohne Kennwort ermöglichen.
  - Die Einstellung `!requiretty` muss definiert sein.
- Berechtigungen zur Ausführung des MongoDB-Standardservermoduls `/usr/local/bin/mongodb`. Diese Berechtigung ist für IBM Spectrum Protect Plus erforderlich, um die `pymongo`-API zum Herstellen der Verbindung zu MongoDB-Servern mithilfe des zugeordneten DNS-/IP-Namens und Ports der Instanz verwenden zu können. Diese Methode wird zum Sammeln von Informationen zu MongoDB-Instanzen und -Datenbanken verwendet.
- Wenn der MongoDB-Server durch die rollenbasierte Authentifizierung geschützt wird, müssen Sie die entsprechenden Berechtigungen festlegen, damit der MongoDB-Agent in Ihrer IBM Spectrum Protect

Plus-Umgebung funktionsfähig ist. Weitere Informationen finden Sie in Kapitel 13, „Benutzerzugriff verwalten”, auf Seite 311. .

Ports

Die folgenden Ports werden von IBM Spectrum Protect Plus-Agentenbenutzern verwendet. Ports, die in der Spalte "Firewallregel" mit Accept angegeben sind, verwenden sichere Verbindungen (HTTPS oder SSL).

Tabelle 13. Eingehende IBM Spectrum Protect Plus-Agentenfirewallverbindungen

Port	Protokoll	Firewallregel	Service	Beschreibung
22	TCP	Accept	SSH	Für die SSH-Datenübertragung zum und vom internen vSnap-Server verwendet

Tabelle 14. Abgehende IBM Spectrum Protect Plus-Agentenfirewallverbindungen

Port	Protokoll	Service	Beschreibung
111	TCP	vSnap RPC Port Bind	Ermöglicht Clients das Erkennen von Ports, die ONC-Clients (ONC = Open Network Computing) für die Kommunikation mit ONC-Servern erfordern
2049	TCP	vSnap NFS	Für die NFS-Dateifreigabe über vSnap verwendet
20048	TCP	vSnap NFS Mount	Stellt vSnap-Dateisysteme auf Clients, wie beispielsweise dem VADP-Proxy, Anwendungsservern und Virtualisierungsdatenspeichern, bereit

Oracle-Anforderungen

Überprüfen Sie die Oracle-Datenbanksicherungs- und -zurückschreibungsanforderungen für IBM Spectrum Protect Plus.

Um sicherzustellen, dass Sicherungs- und Zurückschreibungsoperationen erfolgreich ausgeführt werden können, muss Ihr System die Hardware- und Softwareanforderungen erfüllen. Die folgenden Anforderungen dienen als Ausgangspunkt. Die aktuellen Anforderungen, die unter Umständen Aktualisierungen umfassen, finden Sie in Technote 2013790.

Konfigurationsanforderungen

Datenbankversionen

- Oracle 11g R2

- Oracle 12c R1
- Oracle 12c R2
- Oracle 18c

Anmerkung: Für Multi-Tenant-Datenbanken in Oracle 12c und höher unterstützt IBM Spectrum Protect Plus den Schutz und die Wiederherstellung der Containerdatenbank, einschließlich aller in ihr enthaltenen Plug-in-Datenbanken (PDBs). Die differenzierte Wiederherstellung bestimmter PDBs kann über die Instant Disk Restore-Wiederherstellung in Kombination mit RMAN erfolgen.

Betriebssysteme

- AIX 6.1 TL9 und höhere Wartungs- und Modifikationsstufen
- AIX 7.1 und höhere Wartungs- und Modifikationsstufen
- Red Hat Enterprise Linux/CentOS 6.5 und höhere Wartungs- und Modifikationsstufen
- Red Hat Enterprise Linux/CentOS 7.0 und höhere Wartungs- und Modifikationsstufen
- SUSE Linux Enterprise Server 11.0 SP4 und höhere Wartungs- und Modifikationsstufen
- SUSE Linux Enterprise Server 12.0 SP1 und höhere Wartungs- und Modifikationsstufen
- SUSE Linux Enterprise Server 15.0 und höhere Wartungs- und Modifikationsstufen

Weitere Hinweise

- Oracle DataGuard wird nicht unterstützt.
- Datenbanken müssen sich im Modus ARCHIVELOG befinden. IBM Spectrum Protect Plus kann keine Datenbanken schützen, die im Modus NOARCHIVELOG ausgeführt werden.
- RAC-Datenbankwiederherstellungen (RAC = Real Application Cluster) gelten nicht für Server-Pools. IBM Spectrum Protect Plus kann Datenbanken in einem RAC wiederherstellen, aber nicht in bestimmten Server-Pools.
- RAC-Datenbanken müssen so konfiguriert sein, dass die Position der RMAN-Momentaufnahmesteuerdatei auf gemeinsam genutzten Speicher verweist, auf den alle Clusterinstanzen zugreifen können.
- Wenn eine Oracle-Datenbank zurückgeschrieben wird, die zum Zeitpunkt der Sicherung für Multithreading konfiguriert war, ist die zurückgeschriebene Datenbank eine Nicht-Multithread-Datenbank. Die zurückgeschriebene Datenbank muss manuell für die Verwendung des Multithreading rekonfiguriert werden.

Software

- Die **bash**- und **sudo**-Pakete müssen installiert sein. **sudo** muss Version 1.7.6p2 oder höher haben. Führen Sie **sudo -V** aus, um die Version zu überprüfen.
- Python Version 2.6.x oder 2.7.x muss installiert sein.
- **Nur RHEL/CentOS 6.x.**

  Stellen Sie sicher, dass das Paket `util-linux-ng` aktuell ist, indem Sie **`yum update util-linux-ng`** ausführen.

  Abhängig von Ihrer Version oder Distribution kann das Paket den Namen `util-linux` haben.

Konnektivität

- Der SSH-Service muss an Port 22 auf dem Server aktiv sein und alle Firewalls müssen so konfiguriert sein, dass sie IBM Spectrum Protect Plus das Herstellen der Verbindung zum Server mithilfe von SSH ermöglichen. Das Subsystem SFTP für SSH muss ebenfalls aktiviert sein.
- Der Server kann mithilfe eines DNS-Namens oder einer IP-Adresse registriert werden. DNS-Namen müssen von IBM Spectrum Protect Plus aufgelöst werden können.
- Wenn DNS nicht verfügbar ist, müssen Sie den Server der Datei `/etc/hosts` auf der IBM Spectrum Protect Plus-Appliance unter Verwendung der Befehlszeile hinzufügen.

- Registrieren Sie bei der Registrierung von Oracle RAC-Knoten jeden Knoten unter Verwendung seiner physischen IP-Adresse oder seines physischen Namens. Verwenden Sie keinen virtuellen Namen oder SCAN (Single Client Access Name).

Authentifizierung und Berechtigungen

- Der Oracle Server muss in IBM Spectrum Protect Plus unter Verwendung eines Betriebssystembenutzers, der auf dem Oracle Server vorhanden ist, registriert werden. Der Benutzer wird nachfolgend als IBM Spectrum Protect Plus-Agentenbenutzer bezeichnet.
- Stellen Sie sicher, dass das Kennwort korrekt konfiguriert ist und sich der Benutzer anmelden kann, ohne dass weitere Eingabeaufforderungen, wie beispielsweise Eingabeaufforderungen zum Zurücksetzen des Kennworts, angezeigt werden.

Der IBM Spectrum Protect Plus-Agentenbenutzer muss über die folgenden Berechtigungen verfügen:

- Berechtigungen zur Ausführung von Befehlen als Root und als Oracle-Softwareeigner (beispielsweise `oracle`, `grid`) unter Verwendung von **sudo**. Diese Berechtigungen sind für Tasks wie beispielsweise das Erkennen von Speicherlayouts, das Bereitstellen von Platten und das Aufheben der Bereitstellung von Platten sowie das Verwalten von Datenbanken und ASM erforderlich.
  - Die `sudoers`-Konfiguration muss dem IBM Spectrum Protect Plus-Agentenbenutzer die Ausführung von Befehlen ohne Kennwort ermöglichen.
  - Die Einstellung !requiretty muss definiert sein.
  - Die Einstellung ENV_KEEP muss die Beibehaltung der Umgebungsvariablen ORACLE_HOME und ORACLE_SID ermöglichen.
- Berechtigungen zum Lesen des Oracle-Bestands. Diese Berechtigungen sind für Tasks wie beispielsweise das Erkennen und Erfassen von Informationen zu Oracle-Ausgangsverzeichnissen und -Datenbanken erforderlich.

  Damit dies möglich ist, muss der IBM Spectrum Protect Plus-Agentenbenutzer zur Oracle-Bestandsgruppe gehören, die in der Regel den Namen `oinstall` hat.

Informationen zum Erstellen eines neuen Benutzers mit erforderlichen Berechtigungen finden Sie in „Beispielkonfiguration eines IBM Spectrum Protect Plus-Agentenbenutzers” auf Seite 39.

NFS

Auf dem Oracle-Server muss der native Linux- oder AIX-NFS-Client installiert sein. IBM Spectrum Protect Plus verwendet NFS zum Bereitstellen von Speicherdatenträgern für Sicherungs- und Zurückschreibungsoperationen.

Während der Datenbankzurückschreibung ist die Oracle-Funktion Direct NFS erforderlich. IBM Spectrum Protect Plus aktiviert Direct NFS automatisch, sofern es noch nicht bereits aktiviert ist.

Damit Direct NFS ordnungsgemäß funktioniert, muss der Eigner der ausführbaren Datei `<ORACLE_HOME>/bin/oradism` unter jedem Oracle-Ausgangsverzeichnis ein Root mit setuid-Berechtigungen sein. Dies ist in der Regel vom Oracle-Installationsprogramm vorkonfiguriert; auf bestimmten Systemen hat die Binärdatei jedoch möglicherweise nicht die erforderlichen Berechtigungen. Weitere Informationen finden Sie in dem Dokument Database Startup Failed with Direct NFS auf der Oracle-Support-Website.

Führen Sie die folgenden Befehle aus, um die korrekten Berechtigungen festzulegen:

- `chown root:oinstall <ORACLE_HOME>/bin/oradism`
- `chmod 750 <ORACLE_HOME>/bin/oradism`

Dabei gibt `oinstall` die Gruppe an, die Eigner der Installation ist.

Datenbankerkennung

IBM Spectrum Protect Plus erkennt Oracle-Installationen und -Datenbanken, indem es die Dateien `/etc/oraInst.loc` und `/etc/oratab` sowie die Liste der aktiven Oracle-Prozesse durchsucht. Wenn die Da-

teien nicht an ihrer Standardposition vorhanden sind, muss das Dienstprogramm "locate" auf dem System installiert werden, damit IBM Spectrum Protect Plus nach den Dateien suchen kann.

IBM Spectrum Protect Plus erkennt Datenbanken und ihre Speicherlayouts, indem es die Verbindung zu aktiven Instanzen herstellt und die Positionen der zugehörigen Datendateien, Protokolldateien usw. abfragt. Damit IBM Spectrum Protect Plus Datenbanken während Katalogisierungs- und Kopieroperationen korrekt erkennen kann, müssen sich die Datenbanken im Status "MOUNTED," "READ ONLY" oder "READ WRITE" befinden. IBM Spectrum Protect Plus kann keine beendeten Datenbankinstanzen erkennen oder schützen.

Überwachung geänderter Blöcke

IBM Spectrum Protect Plus erfordert die Aktivierung von Oracle Block Change Tracking (Überwachung geänderter Blöcke) für geschützte Datenbanken, damit Teilsicherungen effizient ausgeführt werden können. Wenn Block Change Tracking (BCT) nicht bereits aktiviert ist, wird es von IBM Spectrum Protect Plus automatisch während des Sicherungsjobs aktiviert.

Um die Position der BCT-Datei anzupassen, müssen Sie die Funktion "Block Change Tracking" manuell aktivieren, bevor Sie einen zugeordneten Sicherungsjob ausführen. Wenn die Funktion automatisch von IBM Spectrum Protect Plus aktiviert wird, wird die Position der BCT-Datei mithilfe der folgenden Regeln bestimmt:

- Wenn der Parameter **db_create_file_dest** definiert ist, wird die BCT-Datei an der durch diesen Parameter angegebenen Position erstellt.
- Wenn der Parameter **db_create_file_dest** nicht definiert ist, wird die BCT-Datei in demselben Verzeichnis wie der Tabellenbereich SYSTEM erstellt.

Protokollsicherung

- Der **cron**-Dämon muss auf dem Anwendungsserver aktiviert sein.
- Der IBM Spectrum Protect Plus-Agentenbenutzer muss über die erforderlichen Berechtigungen zur Verwendung des Befehls **crontab** und zum Erstellen von Cron-Jobs verfügen. Berechtigungen können über die Konfigurationsdatei `cron.allow` erteilt werden.

Beispielkonfiguration eines IBM Spectrum Protect Plus-Agentenbenutzers

Die folgenden Befehle sind Beispiele zum Erstellen und Konfigurieren eines Betriebssystembenutzers, den IBM Spectrum Protect Plus für die Anmeldung beim Oracle-Server verwendet. Die Befehlssyntax kann abhängig von Ihrem Betriebssystemtyp und Ihrer Betriebssystemversion unterschiedlich sein.

- Erstellen Sie den Benutzer, der als der IBM Spectrum Protect Plus-Agentenbenutzer bezeichnet wird: `useradd -m sppagent`
- Legen Sie ein Kennwort fest: `passwd sppagent`.
- Wenn die schlüsselbasierte Authentifizierung verwendet wird, stellen Sie den öffentlichen Schlüssel in die Datei `/home/sppagent/.ssh/authorized_keys` oder - abhängig von Ihrer SSHD-Konfiguration - in die entsprechende Datei und stellen Sie wie folgt sicher, dass das korrekte Eigentumsrecht und die korrekten Berechtigungen definiert sind:

  ```
  chown -R sppagent:sppagent /home/sppagent/.ssh
  chmod 700 /home/sppagent/.ssh
  chmod 600 /home/sppagent/.ssh/authorized_keys
  ```

- Fügen Sie den Benutzer der Oracle-Installation und der Gruppe OSDBA hinzu: `usermod -a -G oinstall,dba sppagent`
- Wenn ASM verwendet wird, fügen Sie den Benutzer auch der Gruppe OSASM hinzu: `usermod -a -G asmadmin sppagent`
- Fügen Sie am Ende Ihrer `sudoers`-Konfigurationsdatei (in der Regel `/etc/sudoers`) die folgenden Zeilen hinzu. Wenn Ihre vorhandene `sudoers`-Datei für den Import von Konfigurationen aus einem an-

deren Verzeichnis (beispielsweise `/etc/sudoers.d`) konfiguriert ist, können Sie die Zeilen auch in eine neue Datei in diesem Verzeichnis stellen:

```
Defaults:sppagent !requiretty
Defaults:sppagent env_keep+="ORACLE_HOME"
Defaults:sppagent env_keep+="ORACLE_SID"
sppagent ALL=(ALL) NOPASSWD:ALL
```

Ports

Die folgenden Ports werden von IBM Spectrum Protect Plus-Agentenbenutzern verwendet. Ports, die in der Spalte "Firewallregel" mit "Accept" angegeben sind, verwenden eine sichere Verbindung (HTTPS oder SSL).

Tabelle 15. Eingehende IBM Spectrum Protect Plus-Agentenfirewallverbindungen

Port	Protokoll	Firewallregel	Service	Beschreibung
22	TCP	Accept	SSH	Für die SSH-Datenübertragung zum und vom internen vSnap-Server verwendet.

Tabelle 16. Abgehende IBM Spectrum Protect Plus-Agentenfirewallverbindungen

Port	Protokoll	Service	Beschreibung
111	TCP	vSnap RPC Port Bind	Ermöglicht Clients das Erkennen von Ports, die ONC-Clients (ONC = Open Network Computing) für die Kommunikation mit ONC-Servern erfordern
443	TCP	HTTPS	Ermöglicht dem Oracle-Server die Kommunikation mit IBM Spectrum Protect Plus zum Senden von Alerts für den Fall, dass Protokollsicherungen fehlschlagen
2049	TCP	vSnap NFS	Für die NFS-Dateifreigabe über vSnap verwendet.
20048	TCP	vSnap NFS Mount	Stellt vSnap-Dateisysteme auf Clients, wie beispielsweise dem VADP-Proxy, Anwendungsservern und Virtualisierungsdatenspeichern, bereit.

Microsoft SQL Server-Anforderungen

Überprüfen Sie die Microsoft SQL Server-Datenbanksicherungs- und -zurückschreibungsanforderungen für IBM Spectrum Protect Plus.

Um sicherzustellen, dass Sicherungs- und Zurückschreibungsoperationen erfolgreich ausgeführt werden können, muss Ihr System die Hardware- und Softwareanforderungen erfüllen. Die folgenden Anforderungen dienen als Ausgangspunkt. Die aktuellen Anforderungen, die unter Umständen Aktualisierungen umfassen, finden Sie in Technote 2013790.

Konfiguration

Datenbankversionen

- SQL Server 2008 R2 SP3
- SQL Server 2012
- SQL Server 2012 SP2
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017

Installieren Sie zur Leistungsoptimierung die neuesten SQL Server-Patchs und -Aktualisierungen in Ihrer Umgebung.

Betriebssysteme

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Windows Remote Shell (WinRM) muss aktiviert sein.

Eine iSCSI-Route muss zwischen dem SQL Server-System und dem vSnap-Server aktiviert werden. Weitere Informationen finden Sie in Microsoft iSCSI Initiator Step-by-Step Guide.

IBM Spectrum Protect Plus-Bestandsjobs erkennen Systemdatenbanken und markieren die Datenbanken, die für den Schutz auswählbar sind. Protokollsicherungen werden für alle Systemdatenbanken und Datenbanken, die im einfachen Wiederherstellungsmodell ausgeführt werden, als nicht auswählbar markiert.

Speicherinterne OLTP

Die speicherinterne Onlinetransaktionsverarbeitung (OLTP = Online Transaction Processing) ist eine speicheroptimierte Datenbanksteuerkomponente zur Verbesserung der Leistung von Datenbankanwendungen. Diese Steuerkomponente wird in SQL Server 2014 und höher unterstützt. Die folgenden Anforderungen und Einschränkungen gelten für die Verwendung der speicherinternen OLTP:

- Die maximale Länge des Pfads der Zurückschreibungsdatei muss weniger als 256 Zeichen betragen. Wenn der ursprüngliche Pfad diese Länge überschreitet, verwenden Sie gegebenenfalls einen angepassten Pfad für die Zurückschreibungsdatei, um die Länge zu reduzieren.
- Die Metadaten, die zurückgeschrieben werden können, unterliegen dem Zurückschreibungsleistungsspektrum von Volume Shadow Copy Service (VSS) und SQL Server.

Teilsicherung

IBM Spectrum Protect Plus verwendet USN-Änderungsjournaltechnologie (USN = Update Sequence Number = Updatesequenznummer) zur Ausführung von Teilsicherungen in einer SQL Server-Umgebung. Das USN-Änderungsjournal stellt Schreibbereichsüberwachung (Schreibbereichnachverfolgung) für einen Datenträger zur Verfügung, wenn die Dateigröße den Schwellenwert für die Mindestdateigröße erreicht. Die

Informationen zum Offset der geänderten Byte und zur Längenerweiterung können für eine bestimmte Datei abgefragt werden.

Die folgende Anforderungen müssen erfüllt sein, um die Schreibbereichsüberwachung zu ermöglichen:

- Windows Server 2012 R2 oder höher
- NTFS Version 3.0 oder höher

Die folgenden Technologien werden für die Überwachung geänderter Byte nicht unterstützt:

- Resilient File System (ReFS)
- Protokoll Server Message Block (SMB) 3.0
- SMB TFO (Transparent Failover)
- SMB 3.0 mit Scale-out-(SO-)Dateifreigaben

Standardmäßig ist für das USN-Änderungsjournaling 512 MB Speicherbereich zugeordnet. Wenn ein Journalüberlauf erkannt wird, wird darüber hinaus eine Journalgröße von 2 GB für die Verwaltung des aktiven Dateisystems zugeordnet.

Der für Spiegelkopiespeicher (Schattenkopiespeicher) erforderliche Mindestspeicherbereich beträgt 100 MB, obwohl auf Systemen mit erhöhter Aktivität unter Umständen mehr Speicherbereich erforderlich ist. Der SQL Server-Agent überprüft den Speicherbereich auf dem Quellendatenträger; eine Sicherung schlägt fehl, wenn der freie Speicherbereich auf dem Quellendatenträger weniger als 100 MB beträgt. Im Jobprotokoll wird eine Warnnachricht angezeigt, wenn der freie Speicherbereich weniger als 10 % beträgt; anschließend wird die Sicherung fortgesetzt.

Eine Basissicherung wird erzwungen, wenn die folgenden Bedingungen erkannt werden:

- Es wird eine Journaldiskontinuität zurückgemeldet, da das Protokoll die maximale Größe erreicht hat, das Journaling inaktiviert wurde oder die katalogisierte USN-ID geändert wurde.
- Die Dateigröße ist kleiner-gleich dem überwachten Schwellenwert, der standardmäßig 1 MB beträgt.
- Eine Datei wird nach einem vorherigen Sicherungsjob hinzugefügt.

Protokollsicherung

Bevor Protokolldateien in das vSnap-Repository kopiert werden, speichert IBM Spectrum Protect Plus unter Verwendung des Sicherungsordners, der für die SQL-Serverinstanz konfiguriert ist, die Sammlung von Protokollen zwischen. Es muss genügend freier Speicherbereich verfügbar sein, um die Transaktionsprotokolle zwischen Sicherungsjobs speichern zu können. Der Staging-Bereich kann geändert werden, indem die Konfiguration des Sicherungsordners mithilfe von SQL Server Management Studio (SSMS) geändert wird.

Um sicherzustellen, dass die SQL Server-Protokollsicherung korrekt ausgeführt werden kann, ist unter Umständen eine Änderung der Windows-Gruppenrichtlinie erforderlich.

Die Gruppenrichtlinienobjekteinstellung (GPO-Einstellung) für die Richtlinie **Netzwerksicherheit: LAN Manager-Authentifizierungsebene**, die sich unter **Computerkonfiguration** > **Windows-Einstellungen** > **Sicherheitseinstellungen** > **Lokale Richtlinien** > **Sicherheitsoptionen** befindet, muss auf eine der folgenden Optionen gesetzt sein:

- **Nicht definiert**
- **Nur NTLMv2-Antworten senden**
- **Nur NTLMv2-Antworten senden. LM verweigern**
- **Nur NTLMv2-Antworten senden. LM NTLM verweigern**

Die Option **Nur NTLM-Antworten senden** ist nicht mit der vSnap-CIFS- oder -SMB-Version kompatibel und kann CIFS-Authentifizierungsprobleme zur Folge haben.

SQL Server AlwaysOn-Verfügbarkeitsgruppen konfigurieren

Konfigurieren Sie die bevorzugte Instanz für Sicherungsoperationen mithilfe von SQL Server Management Studio. Führen Sie die folgenden Schritte aus:

1. Wählen Sie den Knoten **Verfügbarkeitsgruppe** aus.
2. Wählen Sie die Verfügbarkeitsgruppe aus, die konfiguriert werden soll, und wählen Sie dann **Eigenschaften** aus.
3. Wählen Sie im Dialogfenster **Eigenschaften der Verfügbarkeitsgruppe** die Option **Sicherungseinstellungen** aus.

Wählen Sie im Fenster **Wo sollten Sicherungen erfolgen?** eine beliebige Option aus. Wenn sekundäre Replikate bevorzugt werden und mehr als ein sekundäres Replikat verfügbar ist, wählt der IBM Spectrum Protect Plus-Job-Executor das erste sekundäre Replikat in der Liste der bevorzugten Replikate, die vom IBM Spectrum Protect Plus-SQL Server-Agenten zurückgemeldet wird, aus.

Der VSS-Sicherungstyp wird vom SQL Server-Agenten auf COPY_ONLY gesetzt.

Registrierung und Authentifizierung

Registrieren Sie jeden SQL-Server bei IBM Spectrum Protect Plus nach Namen oder nach IP-Adresse. Wenn Sie einen SQL Server-Clusterknoten (AlwaysOn) registrieren, ist jeder Knoten nach Namen oder nach IP-Adresse zu registrieren. Die IP-Adressen müssen öffentlich und an Port 5985 empfangsbereit sein. Der vollständig qualifizierte Domänenname muss von der IBM Spectrum Protect Plus-Appliance aufgelöst und weitergeleitet werden können.

Die Benutzeridentität muss über die erforderlichen Berechtigungen zum Installieren und Starten des IBM Spectrum Protect Plus-Tools-Service auf dem Knoten verfügen, einschließlich des Rechts **Als Service anmelden**. Weitere Informationen finden Sie in dem folgenden Artikel, Add the Log on as a service Right to an Account, auf der Microsoft-Website.

Die Benutzeridentität folgt dem Standardformat *Domäne**Name*, wenn die virtuelle Maschine einer Domäne zugeordnet ist. Das Format *lokaler Administrator* wird verwendet, wenn der Benutzer ein lokaler Administrator ist.

Kerberos

Die Kerberos-basierte Authentifizierung kann aktiviert werden, indem eine Konfigurationsdatei in der IBM Spectrum Protect Plus-Appliance angegeben wird. Durch die Einstellungen wird das standardmäßige Windows-NTLM-Protokoll außer Kraft gesetzt.

Nur für die Kerberos-basierte Authentifizierung muss die Benutzeridentität im Format `Benutzername@FQDN` angegeben werden. Der Benutzername muss sich mit dem registrierten Kennwort authentifizieren können, um ein Ticket-Granting-Ticket (TGT) vom Key-Distribution-Center (KDC) in der Domäne anzufordern, die mit dem vollständig qualifizierten Domänennamen (FQDN) angegeben wird.

Berechtigungen

Der IBM Spectrum Protect Plus-Agentenbenutzer eines SQL-Servers muss die folgenden Berechtigungen haben:

- Die SQL Server-Berechtigungen `public` und `sysadmin`
- Windows-Berechtigung zur lokalen Verwaltung, die für das VSS-Framework und den Datenträger- und Plattenzugriff erforderlich ist
- Berechtigungen für den Zugriff auf Clusterressourcen in einer SQL Server AlwaysOn- und SQL Server-FCI-Umgebung

In jeder SQL Server-Instanz kann ein spezifischer Benutzeraccount für den Zugriff auf die Ressourcen dieser SQL Server-Instanz verwendet werden.

Das SQL Server-VDI-basierte Framework dient zur Interaktion mit SQL Server-Datenbanken und Protokollsicherungs- und Zurückschreibungsoperationen. Eine VDI-Verbindung erfordert die SQL Server-Be-

rechtigung `sysadmin`. Der Eigner der zurückgeschriebenen Datenbank wird nicht in den ursprünglichen Eigner geändert. Ein manueller Schritt ist erforderlich, um den Eigner einer zurückgeschriebenen Datenbank zu ändern. Weitere Informationen zum VDI-Framework VDI enthält der folgende Microsoft-Artikel: SQL Server VDI Backup- und Wiederherstellungsvorgänge erfordern Systemadministratorrechte.

Der SQL Server-Servicezielaccount muss über Berechtigungen für den Zugriff auf SQL Server-Zurückschreibungsdateien verfügen. Siehe "Überlegungen zur Verwaltung" in dem folgenden Microsoft-Artikel: Sichern von Daten- und Protokolldateien.

Der Windows-Taskplaner wird zum Planen von Protokollsicherungen verwendet. Abhängig von der Umgebung empfangen Benutzer unter Umständen den folgenden Fehler: `Eine angegebene Anmeldesitzung ist nicht vorhanden. Sie wurde gegebenenfalls bereits beendet.` Ursache für diesen Fehler ist eine Netzzugriffsgruppenrichtlinieneinstellung, die inaktiviert werden muss. Weitere Informationen zum Inaktivieren dieses Gruppenrichtlinienobjekts (GPO) enthält der folgende Microsoft Support-Artikel: A specified logon session does not exist. It may already have been terminated, error when you try to map to a network drive of a DFS share.

Ports

Die folgenden Ports werden von IBM Spectrum Protect Plus-Agentenbenutzern verwendet. Die Ports, die mit "Accept" angegeben sind, verwenden eine sichere Verbindung (HTTPS oder SSL).

Tabelle 17. Eingehende IBM Spectrum Protect Plus-Agentenfirewallverbindungen

Port	Protokoll	Firewall	Service	Beschreibung
5985	TCP	Accept	WinRM	Windows-Remoteverwaltungsdienst
5986	TCP	Accept	WinRM	Sicherer Windows-Remoteverwaltungsdienst

Tabelle 18. Abgehende IBM Spectrum Protect Plus-Agentenfirewallverbindungen

Port	Protokoll	Service	Beschreibung
3260 Auf diesem Knoten ist der iSCSI-Initiator erforderlich.	TCP	vSnap-iSCSI	iSCSI-vSnap-Zielport, der zur Bereitstellung von LUNs für Sicherungs- und Wiederherstellungsoperationen verwendet wird.
137	UDP	vSnap-SMB/-CIFS	vSnap-SMB-/-CIFS-Zielport, der zur Bereitstellung von Dateisystemfreigaben für Transaktionsprotokollsicherungs- und -wiederherstellungsoperationen verwendet wird.

Tabelle 18. Abgehende IBM Spectrum Protect Plus-Agentenfirewallverbindungen (Forts.)			
Port	**Protokoll**	**Service**	**Beschreibung**
138	UDP	vSnap-SMB/-CIFS	vSnap-SMB-/-CIFS-Zielport, der zur Bereitstellung von Dateisystemfreigaben für Transaktionsprotokollsicherungs- und -wiederherstellungsoperationen verwendet wird.
139	TCP	vSnap-SMB/-CIFS	vSnap-SMB-/-CIFS-Zielport, der zur Bereitstellung von Dateisystemfreigaben für Transaktionsprotokollsicherungs- und -wiederherstellungsoperationen verwendet wird.
443	TCP	HTTPS	Ermöglicht dem SQL-Server die Kommunikation mit IBM Spectrum Protect Plus zum Senden von Alerts für den Fall, dass Protokollsicherungen fehlschlagen.
445	TCP	vSnap-SMB/-CIFS	vSnap-SMB-/-CIFS-Zielport, der zur Bereitstellung von Dateisystemfreigaben für Transaktionsprotokollsicherungs- und -wiederherstellungsoperationen verwendet wird.

IBM Spectrum Protect Plus-Installationspaket abrufen

Sie können das IBM Spectrum Protect Plus-Installationspaket von einer IBM Download-Site, wie beispielsweise Passport Advantage oder Fix Central, abrufen. Diese Pakete enthalten Dateien, die zum Installieren oder Aktualisieren der IBM Spectrum Protect Plus-Komponenten erforderlich sind.

Vorbereitende Schritte

Eine Liste der Installationspakete nach Komponente und die Links zur Download-Site für die Dateien finden Sie in Technote 879861.

Vorgehensweise

Laden Sie die entsprechende Installationsdatei herunter.

Für die Installation auf VMware- und Microsoft Hyper-V-Systemen wird jeweils eine andere Installationsdatei bereitgestellt. Stellen Sie sicher, dass Sie die für Ihre Umgebung korrekte Datei herunterladen.

Wichtig: Übernehmen Sie die Namen der Installations- oder Aktualisierungsdateien unverändert. Die ursprünglichen Dateinamen sind erforderlich, damit der Installations- oder Aktualisierungsprozess fehlerfrei ausgeführt werden kann.

Zugehörige Konzepte

„IBM Spectrum Protect Plus-Komponenten aktualisieren" auf Seite 87
Sie können die virtuelle IBM Spectrum Protect Plus-Appliance, vSnap-Server und die VADP-Proxy-Server aktualisieren, um die neuesten Funktionen und funktionalen Erweiterungen zu erhalten. Software-Patches und -Updates werden mithilfe der Verwaltungskonsole von IBM Spectrum Protect Plus oder mithilfe der Befehlszeilenschnittstelle für diese Komponenten installiert.

Zugehörige Tasks

„IBM Spectrum Protect Plus als virtuelle VMware-Appliance installieren" auf Seite 46
Um IBM Spectrum Protect Plus in einer VMware-Umgebung zu installieren, implementieren Sie eine Open Virtualization Format-Schablone (OVF-Schablone). Durch das Implementieren einer OVF-Schablone wird eine virtuelle Appliance erstellt, die die Anwendung auf einem VMware-Host, wie beispielsweise einem ESXi-Server, enthält.

„IBM Spectrum Protect Plus als virtuelle Hyper-V-Appliance installieren" auf Seite 48
Um IBM Spectrum Protect Plus in einer Microsoft Hyper-V-Umgebung zu installieren, importieren Sie die IBM Spectrum Protect Plus for Hyper-V-Schablone. Durch das Importieren einer Schablone wird eine virtuelle Appliance erstellt, die die Anwendung IBM Spectrum Protect Plus auf einer virtuellen Hyper-V-Maschine enthält. Ein lokaler vSnap-Server, der bereits benannt und registriert ist, wird ebenfalls in der virtuellen Appliance installiert.

„vSnap-Server installieren" auf Seite 55
Wenn Sie eine IBM Spectrum Protect Plus-Appliance implementieren, wird automatisch ein vSnap-Server installiert. Dieser Server ist das primäre Sicherungsziel. In umfangreicheren Unternehmensumgebungen sind unter Umständen weitere vSnap-Server erforderlich.

IBM Spectrum Protect Plus als virtuelle VMware-Appliance installieren

Um IBM Spectrum Protect Plus in einer VMware-Umgebung zu installieren, implementieren Sie eine Open Virtualization Format-Schablone (OVF-Schablone). Durch das Implementieren einer OVF-Schablone wird eine virtuelle Appliance erstellt, die die Anwendung auf einem VMware-Host, wie beispielsweise einem ESXi-Server, enthält.

Vorbereitende Schritte

Führen Sie die folgenden Tasks aus:

- Überprüfen Sie die IBM Spectrum Protect Plus-Systemanforderungen in „Komponentenanforderungen" auf Seite 11 und „Hypervisoranforderungen" auf Seite 23.
- Laden Sie die Schabloneninstallationsdatei der virtuellen Appliance, `CC1QCML.ova`, von Passport Advantage Online herunter. Informationen zum Herunterladen von Dateien finden Sie in Technote 879861.
- Überprüfen Sie in der heruntergeladenen Schabloneninstallationsdatei die MD5-Kontrollsumme. Stellen Sie sicher, dass die generierte Kontrollsumme mit der bereitgestellten Kontrollsumme in der MD5-Kontrollsummendatei, die Teil des Software-Downloads ist, übereinstimmt.
- Während der Implementierung werden Sie zur Eingabe der Netzeigenschaften in der VMware-Benutzerschnittstelle aufgefordert. Sie können die Konfiguration einer statischen IP-Adresse eingeben oder alle Felder leer lassen, um eine DHCP-Konfiguration zu verwenden.
- Um nach der Implementierung eine neue statische IP-Adresse zuzuordnen, können Sie das Tool NetworkManager Text User Interface (nmtui) verwenden. Weitere Informationen finden Sie in „Statische IP-Adresse zuordnen" auf Seite 50.

Beachten Sie die folgenden Hinweise:

- Unter Umständen müssen Sie einen IP-Adresspool konfigurieren, der dem VM-Netz zugeordnet ist, in dem IBM Spectrum Protect Plus implementiert werden soll. Die korrekte Konfiguration des IP-Adresspools umfasst das Festlegen des IP-Adressbereichs (sofern verwendet), der Netzmaske, des Gateways, der DNS-Suchzeichenfolge und einer IP-Adresse des DNS-Servers.

- Wenn sich der Hostname der IBM Spectrum Protect Plus-Appliance nach der Implementierung ändert (entweder durch einen Benutzereingriff oder wenn eine neue IP-Adresse über DNS angefordert wird), muss die IBM Spectrum Protect Plus-Appliance erneut gestartet werden.
- Vor der Implementierung muss ein Standardgateway korrekt konfiguriert werden. Mehrere DNS-Zeichenfolgen werden unterstützt und müssen durch Kommas ohne Leerzeichen voneinander getrennt werden.
- Bei höheren Versionen von vSphere ist unter Umständen der vSphere Web Client erforderlich, um IBM Spectrum Protect Plus-Appliances zu implementieren.
- IBM Spectrum Protect Plus wurde nicht für IPv6-Umgebungen getestet.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um IBM Spectrum Protect Plus als virtuelle Appliance zu installieren:

1. Implementieren Sie IBM Spectrum Protect Plus, indem Sie eine der folgenden Aktionen ausführen:
   a) Wenn Sie vSphere Client verwenden, klicken Sie im Menü **Aktionen** auf **OVF-Vorlage bereitstellen**.
   b) Wenn Sie vSphere Web Client verwenden, klicken Sie auf **VM erstellen/registrieren** und wählen Sie dann **Virtuelle Maschine aus einer OVF- oder OVA-Datei bereitstellen** aus.
2. Wählen Sie eine ESXi-Ressource aus, um die virtuelle Appliance auszuführen. Klicken Sie auf **Weiter**.
3. Überprüfen Sie die Details. Klicken Sie auf **Weiter**.

   Wichtig:

   Wenn Sie vSphere Web Client verwenden, stellen Sie sicher, dass für die zusätzliche Konfiguration `disk.enableUUID = true` angegeben ist. Wenn dies nicht der Fall ist oder wenn Sie vSphere Client verwenden, fahren Sie mit den Installationsschritten fort und aktivieren Sie diese Option zu einem späteren Zeitpunkt in vSphere Web Client.
4. Geben Sie die Postion der Datei `CC1QCML.ova` an und wählen Sie die Datei aus. Klicken Sie auf **Weiter**.
5. Geben Sie einen aussagekräftigen Namen für die Schablone ein, der zum Namen Ihrer virtuellen Maschine wird. Geben Sie eine geeignete Position zum Implementieren der virtuellen Maschine an. Klicken Sie auf **Weiter**.
6. Wählen Sie den Speicher aus, in dem die virtuelle Appliance installiert werden soll. Der Datenspeicher dieses Speichers muss mit dem Zielhost konfiguriert werden. Die Konfigurationsdatei der virtuellen Appliance und die virtuellen Plattendateien werden in diesem Speicher gespeichert. Stellen Sie sicher, dass der Speicher groß genug ist, um die virtuelle Appliance einschließlich der ihr zugeordneten virtuellen Plattendateien aufnehmen zu können. Wählen Sie ein Plattenformat für die virtuellen Platten aus. Thick Provisioning ermöglicht eine bessere Leistung der virtuellen Appliance. Thin Provisioning verwendet weniger Plattenspeicher zu Lasten der Leistung. Klicken Sie auf **Weiter**.
7. Informieren Sie sich über die Schablonendetails und akzeptieren Sie die Endbenutzerlizenzvereinbarung. Wählen Sie für vSphere Client die Option zum Akzeptieren aller Lizenzvereinbarungen (**I accept all license agreements**) aus oder klicken Sie für vSphere Web Client auf die Option zum Akzeptieren (**Accept**). Klicken Sie auf **Weiter**.
8. Wählen Sie die Netze aus, die für die implementierte Schablone verwendet werden sollen. Wenn Sie auf **Zielnetzwerke** klicken, werden gegebenenfalls mehrere Netze auf dem ESXi-Server als verfügbare Netze angezeigt. Wählen Sie ein Zielnetz aus, das Ihnen die Definition der geeigneten IP-Adresszuordnung für die Implementierung der virtuellen Maschine ermöglicht. Klicken Sie auf **Weiter**.
9. Geben Sie bei vSphere Web Client die Eigenschaftswerte für die virtuelle Appliance ein: DNS, Standardgateway, Domäne, IP-Netzadresse und Netzpräfix. Eine statische IP-Adresse kann angegeben werden. Wird sie nicht angegeben, wird eine von einem DHCP-Server zugeordnete dynamische IP-Adresse verwendet. Das Netzpräfix muss unter Verwendung der CIDR-Notation (CIDR = Classless Inter-Domain Routing) eingegeben werden; gültige Werte sind 1 bis 24. Klicken Sie auf **Weiter**.

Anmerkung: Bei vSphere Client können diese Eigenschaften mithilfe des Tools NetworkManager Text User Interface (`nmtui`) konfiguriert werden. Darüber hinaus können Informationen für das Feld für die Suchdomäne mithilfe dieses Befehls hinzugefügt werden. Weitere Informationen finden Sie in Statische IP-Adresse zuordnen.

10. Überprüfen Sie Ihre Schabloneneinstellungen. Klicken Sie auf **Beenden**, um den Assistenten zu verlassen und die Implementierung der OVF-Schablone zu starten.
11. Nachdem die OVF-Schablone implementiert wurde, schalten Sie Ihre neu erstellte VM ein. Sie können die VM über vSphere Client einschalten.

    Wichtig: Warten Sie mehrere Minuten, damit IBM Spectrum Protect Plus vollständig initialisiert werden kann.

Nächste Schritte
Nachdem die virtuelle Appliance implementiert wurde, werden die Anwendung IBM Spectrum Protect Plus sowie ein lokaler vSnap-Server, der in die Anwendung integriert ist, registriert und automatisch in der virtuellen Appliance installiert. Um IBM Spectrum Protect Plus zu starten, führen Sie die folgenden Aktionen aus:

Aktion	Vorgehensweise
Stellen Sie die Verbindung zur Konsole der virtuellen IBM Spectrum Protect Plus-Appliance mithilfe von VMware Remote Console oder SSH her. Definieren Sie mithilfe von NetworkManager Text User Interface (`nmtui`) Netzkonfigurationen.	Siehe Statische IP-Adresse zuordnen.
Laden Sie den Produktschlüssel hoch.	Siehe „Produktschlüssel hochladen” auf Seite 51.
Starten Sie IBM Spectrum Protect Plus in einem unterstützten Web-Browser.	Siehe „IBM Spectrum Protect Plus starten” auf Seite 73.

IBM Spectrum Protect Plus als virtuelle Hyper-V-Appliance installieren

Um IBM Spectrum Protect Plus in einer Microsoft Hyper-V-Umgebung zu installieren, importieren Sie die IBM Spectrum Protect Plus for Hyper-V-Schablone. Durch das Importieren einer Schablone wird eine virtuelle Appliance erstellt, die die Anwendung IBM Spectrum Protect Plus auf einer virtuellen Hyper-V-Maschine enthält. Ein lokaler vSnap-Server, der bereits benannt und registriert ist, wird ebenfalls in der virtuellen Appliance installiert.

Vorbereitende Schritte
Führen Sie die folgenden Tasks aus:

- Überprüfen Sie die IBM Spectrum Protect Plus-Systemanforderungen in „Komponentenanforderungen” auf Seite 11 und „Hypervisoranforderungen” auf Seite 23.
- Laden Sie die Installationsdatei `CC1QDML.exe` von Passport Advantage Online herunter. Informationen zum Herunterladen von Dateien finden Sie in Technote 879861.
- Überprüfen Sie weitere Hyper-V-Systemanforderungen. Siehe Systemanforderungen für Hyper-V unter Windows Server.
- Überprüfen Sie in der heruntergeladenen Schabloneninstallationsdatei die MD5-Kontrollsumme. Stellen Sie sicher, dass die generierte Kontrollsumme mit der bereitgestellten Kontrollsumme in der MD5-Kontrollsummendatei, die Teil des Software-Downloads ist, übereinstimmt.
- Wenn sich der Hostname der virtuellen IBM Spectrum Protect Plus-Appliance nach der Implementierung ändert (entweder durch einen Benutzereingriff oder wenn eine neue IP-Adresse über DNS angefordert wird), muss die virtuelle IBM Spectrum Protect Plus-Appliance erneut gestartet werden.

- Für alle Hyper-V-Server, einschließlich Clusterknoten, muss der Microsoft-iSCSI-Initiator-Dienst in den zugehörigen Listen "Dienste" aktiv sein. Setzen Sie den Starttyp dieses Dienstes auf "Automatisch", damit die Ausführung des Dienstes gestartet wird, wenn der Server gestartet wird.
- Unter Umständen sind Administratorrechte erforderlich, um bestimmte Schritte während des Installationsprozesses ausführen zu können.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um IBM Spectrum Protect Plus als virtuelle Appliance zu installieren:

1. Kopieren Sie die Datei `CC1QDML.exe` auf Ihren Hyper-V-Server.
2. Öffnen Sie das Installationsprogramm und führen Sie den Installationsassistenten aus.
3. Öffnen Sie Hyper-V-Manager und wählen Sie den erforderlichen Server aus.
4. Klicken Sie in Hyper-V-Manager im Fenster **Aktionen** auf **Virtuellen Computer importieren**. Der Assistent "Virtuellen Computer importieren" wird geöffnet. Klicken Sie auf **Weiter**.
5. Klicken Sie im Schritt **Ordner suchen** auf **Durchsuchen...** und navigieren Sie zu dem Ordner, der während der Installation angegeben wurde. Wählen Sie den Ordner mit der Angabe **SPP-{Release}** aus. Klicken Sie auf **Weiter**.
6. Stellen Sie im Schritt **Virtuellen Computer auswählen** sicher, dass die virtuelle Maschine **SPP-{Release}** ausgewählt ist, und klicken Sie dann auf **Weiter**. Das Dialogfenster **Importtyp auswählen** wird geöffnet.
7. Wählen Sie im Schritt **Importtyp auswählen** die Option **Virtuellen Computer direkt registrieren (die vorhandene eindeutige ID verwenden)** aus. Klicken Sie auf **Weiter**.

   Wichtig: Importieren Sie nicht mehrere virtuelle IBM Spectrum Protect Plus-Appliances auf einen einzigen Hyper-V-Server.
8. Setzen Sie im Schritt **Netzwerk verbinden** die Verbindung auf den virtuellen Switch, der verwendet werden soll. Klicken Sie auf **Weiter**.
9. Überprüfen Sie im Schritt **Zusammenfassung** die Beschreibung. Klicken Sie auf **Fertigstellen**, um den Assistenten "Virtuellen Computer importieren" zu schließen.
10. Lokalisieren Sie in Hyper-V-Manager die neue virtuelle Maschine mit dem Namen **SPP-{Release}**. Klicken Sie mit der rechten Maustaste auf diese virtuelle Maschine und klicken Sie auf **Einstellungen**.
11. Das Dialogfenster mit den Einstellungen für diese virtuelle Maschine wird geöffnet. Klicken Sie im linken Teilfenster auf **Hardware > IDE-Controller 0 > Festplatte**.
12. Stellen Sie im Abschnitt "Medien" sicher, dass die korrekte virtuelle Festplatte ausgewählt ist. Notieren Sie den Dateinamen der ursprünglichen virtuellen Platte. Klicken Sie auf **Bearbeiten**.
13. Der Assistent zum Bearbeiten virtueller Festplatten wird geöffnet. Rufen Sie den Schritt **Aktion auswählen** auf.
14. Klicken Sie im Schritt **Aktion auswählen** auf **Konvertieren** und klicken Sie dann auf **Weiter**.
15. Stellen Sie im Schritt **Datenträgerformat auswählen** sicher, dass **VHDX** ausgewählt ist. Klicken Sie auf **Weiter**.
16. Klicken Sie im Schritt **Datenträgertyp auswählen** auf **Feste Größe**. Klicken Sie auf **Weiter**.
17. Lokalisieren Sie für den Schritt **Datenträger konfigurieren** den Ordner, in dem die Datei für virtuelle Datenträger (virtuelle Plattendatei) der virtuellen IBM Spectrum Protect Plus-Appliance gespeichert werden soll. Verwenden Sie denselben Dateinamen, der in Schritt 12 notiert wurde. Wenn dasselbe Installationsverzeichnis wie in Schritt 2 wiederverwendet wird, verwenden Sie einen anderen Namen. Klicken Sie auf **Weiter**.

    Wichtig: Stellen Sie sicher, dass das Plattenlaufwerk, in dem sich der Ordner befindet, über genügend Plattenspeicher verfügt, um die Datei für virtuelle Datenträger mit fester Größe aufnehmen zu können.
18. Überprüfen Sie im Schritt **Zusammenfassung** die Beschreibung. Klicken Sie auf **Fertigstellen**, um den Assistenten zum Bearbeiten virtueller Festplatten zu schließen und die Konvertierung der virtuel-

len Platte zu starten. Nachdem der Prozess abgeschlossen ist, kann die ursprüngliche Datei für virtuelle Festplatte gelöscht werden.

19. Klicken Sie im Dialog mit den Einstellungen für die virtuelle Maschine auf **Durchsuchen**. Öffnen Sie die neu erstellte Datei für virtuelle Festplatte (VHDX-Datei), die im vorherigen Schritt erstellt wurde.
20. Wiederholen Sie die Schritte 12 bis 19 für jede Festplatte unter **Hardware > SCSI-Controller**. Klicken Sie auf **OK**, um den Dialog mit den Einstellungen zu schließen.
21. Klicken Sie in Hyper-V-Manager mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Starten**.
22. Ermitteln Sie mithilfe von Hyper-V-Manager die IP-Adresse der neuen virtuellen Maschine, sofern die Adresse automatisch zugeordnet wurde. Um einer virtuellen Maschine eine statische IP-Adresse zuzuordnen, verwenden Sie das Tool NetworkManager Text User Interface (`nmtui`).

    Weitere Informationen finden Sie in „Statische IP-Adresse zuordnen” auf Seite 50.

Nächste Schritte

Führen Sie nach der Installation der virtuellen Appliance die folgenden Aktionen aus:

Aktion	Vorgehensweise
Starten Sie die virtuelle Appliance erneut.	Ziehen Sie die Dokumentation für die virtuelle Appliance zu Rate.
Laden Sie den Produktschlüssel hoch.	Siehe „Produktschlüssel hochladen” auf Seite 51.
Starten Sie IBM Spectrum Protect Plus in einem unterstützten Web-Browser.	Siehe „IBM Spectrum Protect Plus starten” auf Seite 73.

Statische IP-Adresse zuordnen

Um nach der Erstimplementierung eine neue statische IP-Adresse zuzuordnen, kann ein Netzadministrator mithilfe des Tools NetworkManager Text User Interface (`nmtui`) eine statische IP-Adresse zuordnen. Zur Ausführung von nmtui sind sudo-Berechtigungen erforderlich.

Vorgehensweise

Um eine neue statische IP-Adresse zuzuordnen, müssen Sie sicherstellen, dass die virtuelle IBM Spectrum Protect Plus-Maschine eingeschaltet ist; außerdem müssen Sie die folgenden Schritte ausführen:

1. Melden Sie sich bei der Konsole der virtuellen Maschine mit der Benutzer-ID **serveradmin** an.

   Das Anfangskennwort ist `sppDP758`.
2. Geben Sie in einer CentOS-Befehlszeile `nmtui` ein, um die Schnittstelle zu öffnen.
3. Wählen Sie im Hauptmenü **Edit a connection** aus und klicken Sie dann auf **OK**.
4. Wählen Sie die Netzverbindung aus und klicken Sie dann auf **Edit**.
5. Geben Sie in der Anzeige **Edit Connection** eine verfügbare statische IP-Adresse ein, die noch nicht im Gebrauch ist.
6. Speichern Sie die Konfiguration der statischen IP-Adresse, indem Sie auf **OK** klicken; starten Sie dann die IBM Spectrum Protect Plus-Appliance erneut.

Zugehörige Tasks

„IBM Spectrum Protect Plus als virtuelle VMware-Appliance installieren” auf Seite 46
Um IBM Spectrum Protect Plus in einer VMware-Umgebung zu installieren, implementieren Sie eine Open Virtualization Format-Schablone (OVF-Schablone). Durch das Implementieren einer OVF-Schablone wird eine virtuelle Appliance erstellt, die die Anwendung auf einem VMware-Host, wie beispielsweise einem ESXi-Server, enthält.

„IBM Spectrum Protect Plus als virtuelle Hyper-V-Appliance installieren” auf Seite 48
Um IBM Spectrum Protect Plus in einer Microsoft Hyper-V-Umgebung zu installieren, importieren Sie die IBM Spectrum Protect Plus for Hyper-V-Schablone. Durch das Importieren einer Schablone wird eine vir-

tuelle Appliance erstellt, die die Anwendung IBM Spectrum Protect Plus auf einer virtuellen Hyper-V-Maschine enthält. Ein lokaler vSnap-Server, der bereits benannt und registriert ist, wird ebenfalls in der virtuellen Appliance installiert.

Produktschlüssel hochladen

IBM Spectrum Protect Plus wird für einen begrenzten Zeitraum im Auswertungsmodus ausgeführt. Ein gültiger Produktschlüssel ist erforderlich, um die Ausführung von IBM Spectrum Protect Plus-Funktionen ohne zeitliche Begrenzung zu ermöglichen.

Vorbereitende Schritte
Speichern Sie den Produktschlüssel auf einem Computer mit Internetzugriff und notieren Sie die Position des Schlüssels.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den Produktschlüssel hochzuladen:

1. Geben Sie in einem unterstützten Browser die folgende URL ein:

   ```
   https://HOSTNAME:8090/
   ```

   Dabei ist *HOSTNAME* die IP-Adresse der virtuellen Maschine, auf der die Anwendung implementiert ist.
2. Wählen Sie im Anmeldefenster **Authentifizierungstyp** > **System** aus. Geben Sie die Benutzer-ID `serveradmin` für den Zugriff auf die Verwaltungskonsole ein. Das Standardkennwort ist `sppDP758`.

   Bei der ersten Anmeldung werden Sie zur Eingabe eines neuen Kennworts für den Zugriff auf die Verwaltungskonsole aufgefordert.
3. Klicken Sie auf **Lizenzen verwalten**.
4. Klicken Sie auf **Datei auswählen** und suchen Sie dann auf Ihrem Computer nach dem Produktschlüssel.
5. Klicken Sie auf **Neue Lizenz hochladen**.
6. Klicken Sie auf **Abmelden**.

Nächste Schritte
Führen Sie nach dem Hochladen des Produktschlüssels die folgende Aktion aus:

Aktion	Vorgehensweise
Starten Sie IBM Spectrum Protect Plus in einem unterstützten Web-Browser.	Siehe „IBM Spectrum Protect Plus starten” auf Seite 73.

Firewall-Ports editieren

Verwenden Sie die bereitgestellten Beispiele als Referenz, um Firewall-Ports auf fernen VADP-Proxy-Servern oder Anwendungsservern zu öffnen. Sie müssen den Portdatenverkehr auf das erforderliche Netz oder die erforderlichen Adapter beschränken.

Red Hat Enterprise Linux 7 und höher sowie CentOS 7 und höher

Ports auf fernen VADP-Proxy-Servern oder Anwendungsservern öffnen

Verwenden Sie den folgenden Befehl, um die offenen Ports aufzulisten:

```
firewall-cmd --list-ports
```

Verwenden Sie den folgenden Befehl, um Zonen aufzulisten:

```
firewall-cmd --get-zones
```

Verwenden Sie den folgenden Befehl, um die Zone aufzulisten, die den Ethernet-Port `eth0` enthält:

```
firewall-cmd --get-zone-of-interface=eth0
```

Verwenden Sie den folgenden Befehl, um Port *8098* für den TCP-Datenverkehr zu öffnen. Dieser Befehl ist nicht permanent.

```
firewall-cmd --add-port 8098/tcp
```

Verwenden Sie den folgenden Befehl, um Port *8098* nach dem Neustart der Firewallregeln für den TCP-Datenverkehr zu öffnen. Verwenden Sie diesen Befehl, um die Änderungen permanent zu machen:

```
firewall-cmd --permanent --add-port 8098/tcp
```

Verwenden Sie den folgenden Befehl, um die Änderung am Port rückgängig zu machen:

```
firewall-cmd --remove-port 8098/tcp
```

Verwenden Sie den folgenden Befehl, um einen Bereich von Ports zu öffnen:

```
firewall-cmd --permanent --add-port 60000-61000/tcp
```

Verwenden Sie den folgenden Befehl, um die Firewallregeln mit den Firewallaktualisierungen erneut zu laden:

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

SUSE Linux Enterprise Server 12

Editieren Sie die erweiterten Sicherheitsfirewalloptionen in SUSE Linux Enterprise Server 12 über das Menü **Sicherheit und Benutzer**. Geben Sie den neuen erforderlichen Portbereich an und wenden Sie die Änderungen an.

Firewallkonfigurationen, die IP-Tabellen verwenden

Das Dienstprogramm `iptables` ist in den meisten Linux-Distributionen für die Aktivierung von Firewallregeln und Richtlinieneinstellungen verfügbar. Diese Linux-Distributionen umfassen Red Hat Enterprise Linux 6.8, Red Hat Enterprise Linux 7 und höher, CentOS 7 und höher sowie SUSE Linux Enterprise Server 12. Überprüfen Sie vor der Verwendung dieser Befehle, welche Firewallzonen standardmäßig aktiviert sind. Abhängig von der Zonenkonfiguration müssen die Begriffe INPUT und OUTPUT möglicherweise umbenannt werden, um einer Zone für die erforderliche Regel zu entsprechen.

Für Red Hat Enterprise Linux 7 und höher siehe die folgenden Beispielbefehle:

Verwenden Sie den folgenden Befehl, um die aktuellen Firewallrichtlinien aufzulisten:

```
sudo iptables -S sudo iptables -L
```

Verwenden Sie den folgenden Befehl, um Port *8098* für den eingehenden TCP-Datenverkehr aus dem internen Teilnetz *<172.31.1.0/24>* zu öffnen:

```
sudo iptables -A INPUT -p tcp -s 172.31.1.0/24 --dport 8098 -j ACCEPT
```

Verwenden Sie den folgenden Befehl, um Port *8098* für den abgehenden TCP-Datenverkehr in das interne Teilnetz *<172.31.1.0/24>* zu öffnen:

```
sudo iptables -A OUTPUT -p tcp -d 172.31.1.0/24 --sport 8098 -j ACCEPT
```

Verwenden Sie den folgenden Befehl, um Port *8098* für den abgehenden TCP-Datenverkehr in das externe Teilnetz *<10.11.1.0/24>* ausschließlich für den Ethernet-Port-Adapter `eth1` zu öffnen:

```
sudo iptables -A OUTPUT -o eth1 -p tcp -d 10.11.1.0/24 --sport 8098 -j ACCEPT
```

Verwenden Sie den folgenden Befehl, um Port *8098* für den eingehenden TCP-Datenverkehr für einen Bereich von CES-IP-Adressen (10.11.1.5 bis 10.11.1.11) ausschließlich für den Ethernet-Port-Adapter `eth1` zu öffnen:

```
sudo iptables -A INPUT -i eth1 -p tcp -m iprange --dst-range
10.11.1.5-10.11.1.11 --dport 8098 -j ACCEPT
```

Verwenden Sie den folgenden Befehl, um dem Ethernet-Port-Adapter `eth1` des internen Netzes die Kommunikation mit dem Ethernet-Port-Adapter `eth0` des externen Netzes zu ermöglichen:

`sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT`. Dieses Beispiel gilt speziell für Red Hat Enterprise Linux 7 und höher.

Verwenden Sie den folgenden Befehl, um Port *8098* für den eingehenden Datenverkehr aus dem Teilnetz *10.18.0.0/24* an Ethernet-Port `eth1` in der öffentlichen Zone zu öffnen:

```
iptables -A IN_public_allow -i eth1 -p tcp -s 10.18.0.0/24 --dport 8098 -j AC-
CEPT
```

Verwenden Sie den folgenden Befehl, um die Änderungen an den Firewallregeln zu speichern, damit sie nach einem Neustartprozess für die Firewall erhalten bleiben:

```
sudo iptables-save
```

Verwenden Sie den folgenden Befehl, um UFW (Uncomplicated Firewall) zu zu stoppen und zu starten:

```
service iptables stop service iptables start
```

Kapitel 3. vSnap-Server installieren und konfigurieren

Für jede Installation von IBM Spectrum Protect Plus ist mindestens ein vSnap-Server erforderlich, der das primäre Sicherungsziel darstellt.

Sowohl in der VMware- als auch in der Hyper-V-Umgebung wird ein vSnap-Server mit dem Namen 'localhost' bei der ersten Implementierung der IBM Spectrum Protect Plus-Appliance automatisch installiert. Ein integrierter vSnap-Server befindet sich in einer Partition der IBM Spectrum Protect Plus-Appliance und wird in IBM Spectrum Protect Plus registriert und initialisiert. In kleinen Sicherungsumgebungen reicht der vSnap-Server möglicherweise aus.

In großen Unternehmensumgebungen könnten jedoch weitere vSnap-Server erforderlich sein. Anweisungen zur Festlegung der Anzahl Komponenten sowie zur Erstellung und Integration von vSnap-Servern und anderen Komponenten in Ihrer IBM Spectrum Protect Plus-Umgebung finden Sie in den IBM Spectrum Protect Plus Blueprints.

Zusätzliche vSnap-Server können in virtuellen oder physischen Appliances jederzeit nach der Installation und Implementierung der IBM Spectrum Protect Plus-Appliance installiert werden. Nach der Installation müssen für diese Standalone-vSnap-Server einige Registrierungs- und Konfigurationsschritte ausgeführt werden.

Ein Standalone-vSnap-Server wird wie folgt konfiguriert:

1. Installieren Sie den vSnap-Server.
2. Fügen Sie den vSnap-Server als Plattenspeicher in IBM Spectrum Protect Plus hinzu.
3. Initialisieren Sie das System und erstellen Sie einen Speicherpool.

vSnap-Server installieren

Wenn Sie eine IBM Spectrum Protect Plus-Appliance implementieren, wird automatisch ein vSnap-Server installiert. Dieser Server ist das primäre Sicherungsziel. In umfangreicheren Unternehmensumgebungen sind unter Umständen weitere vSnap-Server erforderlich.

Vorbereitende Schritte

Führen Sie die folgenden Schritte aus:

1. Überprüfen Sie die vSnap-Systemanforderungen in „Komponentenanforderungen” auf Seite 11.
2. Laden Sie das Installationspaket herunter. Für die Installation auf physischen oder virtuellen Maschinen werden unterschiedliche Installationsdateien bereitgestellt. Stellen Sie sicher, dass Sie die für Ihre Umgebung korrekten Dateien herunterladen. Weitere Informationen zum Herunterladen von Dateien finden Sie in Technote 879861.

Physischen vSnap-Server installieren

Ein Linux-Betriebssystem, das physische vSnap-Installationen unterstützt, ist erforderlich, um einen vSnap-Server auf einer physischen Maschine zu installieren.

Vorgehensweise

1. Installieren Sie ein Linux-Betriebssystem, das physische vSnap-Installationen unterstützt. Eine Übersicht über die unterstützten Betriebssysteme finden Sie in „Installationsanforderungen für den physischen vSnap-Server” auf Seite 16.

© Copyright IBM Corp. 2017, 2019

Die Mindestinstallationskonfiguration ist ausreichend, Sie können jedoch auch zusätzliche Pakete, einschließlich einer grafischen Benutzerschnittstelle (GUI), installieren. Die Rootpartition muss nach der Installation über mindestens 8 GB freien Speicherbereich verfügen.

2. Editieren Sie die Datei `/etc/selinux/config`, um den SELinux-Modus in "Permissive" zu ändern.
3. Führen Sie `setenforce 0` aus, um die Einstellung sofort ohne erforderlichen Neustart anzuwenden.
4. Laden Sie die vSnap-Installationsdatei `CC1QGML.run` von Passport Advantage Online herunter. Informationen zum Herunterladen von Dateien finden Sie in Technote 879861.
5. Ändern Sie die Datei mit dem Befehl `chmod +x` *`Dateiname`*`.run` in eine ausführbare Datei und führen Sie diese anschließend aus. Die vSnap-Pakete sowie alle erforderlichen Komponenten werden installiert.

Nächste Schritte

Führen Sie nach der Installation des vSnap-Servers die folgende Aktion aus:

Aktion	Vorgehensweise
Fügen Sie den vSnap-Server IBM Spectrum Protect Plus hinzu und konfigurieren Sie die vSnap-Umgebung.	Siehe „vSnap-Server verwalten” auf Seite 59.

Virtuellen vSnap-Server und einen VADP-Proxy in einer VMware-Umgebung installieren

Um einen virtuellen vSnap-Server und einen vStorage API for Data Protection-Proxy (VADP-Proxy) in einer VMware-Umgebung zu installieren, implementieren Sie eine Open Virtualization Format-Schablone (OVF-Schablone). Damit wird eine Maschine erstellt, die den vSnap-Server und den VADP-Proxy enthält.

Vorbereitende Schritte

Um die Netzverwaltung zu erleichtern, verwenden Sie für die virtuelle Maschine eine statische IP-Adresse. Ordnen Sie die Adresse mithilfe des Tools NetworkManager Text User Interface (nmtui) zu. Anweisungen finden Sie in „Statische IP-Adresse zuordnen” auf Seite 50. Konfigurieren Sie Netzeigenschaften zusammen mit Ihrem Netzadministrator.

Vorgehensweise

1. Laden Sie die Server- und Proxy-Schabloneninstallationsdatei `CC1QEML.ova` von Passport Advantage Online herunter. Informationen zum Herunterladen von Dateien finden Sie in Technote 879861.
2. Um den vSnap-Server zu implementieren, führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie vSphere Client für die Implementierung des vSnap-Servers verwenden, klicken Sie im Menü **Datei** auf **OVF-Vorlage bereitstellen**.
   - Wenn Sie vSphere Web Client verwenden, klicken Sie auf **VM erstellen/registrieren** und dann auf **Virtuelle Maschine aus einer OVF- oder OVA-Datei bereitstellen**. Klicken Sie auf **Weiter**.
3. Geben Sie die Postion der Datei `CC1QEML.ova` an und wählen Sie die Datei aus. Klicken Sie auf **Weiter**.
4. Überprüfen Sie die Schablonendetails und akzeptieren Sie die Endbenutzerlizenzvereinbarung. Klicken Sie auf **Weiter**.
5. Geben Sie einen aussagekräftigen Namen für die Schablone ein, der zum Namen Ihrer virtuellen Maschine wird. Geben Sie eine geeignete Position zum Implementieren der virtuellen Maschine an. Klicken Sie auf **Weiter**.
6. Geben Sie das Datencenter, den Server und den Ressourcenpool für die Implementierung an. Wenn Sie zur Auswahl des Speichers aufgefordert werden, treffen Sie eine Auswahl aus den Datenspeichern, die bereits auf dem Zielhost konfiguriert sind. Die Konfigurationsdatei der virtuellen Maschine und die virtuellen Plattendateien sind im Datenspeicher gespeichert. Wählen Sie einen Datenspeicher aus, der groß genug ist, um die virtuelle Maschine und alle zugehörigen virtuellen Plattendateien aufnehmen zu können. Klicken Sie auf **Weiter**.
7. Wählen Sie ein Plattenformat zum Speichern der virtuellen Platten aus. Zur Leistungsoptimierung können Sie Thick Provisioning auswählen; diese Option ist bereits vorausgewählt. Thin Provisioning

erfordert weniger Plattenspeicher, kann sich jedoch auf die Leistung auswirken. Klicken Sie auf **Weiter**.

8. Wählen Sie die Netze aus, die für die implementierte Schablone verwendet werden sollen. Wenn Sie auf "Zielnetzwerke" klicken, werden gegebenenfalls mehrere Netze auf dem ESX-Server als verfügbare Netze angezeigt. Wählen Sie ein Zielnetz aus, das Ihnen die Definition der geeigneten IP-Adresszuordnung für die Implementierung der virtuellen Maschine ermöglicht. Klicken Sie auf **Weiter**.
9. Geben Sie die Netzeigenschaften für das Standardgateway der virtuellen Maschine, das DNS, die Suchdomäne, die IP-Adresse, das Netzpräfix und den Maschinenhostnamen ein. Wenn Sie eine DHCP-Konfiguration (DHCP = Dynamic Host Configuration Protocol) verwenden, lassen Sie alle Felder leer.

   Einschränkung: Vor der Implementierung der OVF-Schablone muss ein Standardgateway korrekt konfiguriert werden. Mehrere DNS-Zeichenfolgen werden unterstützt und müssen durch Kommas ohne Leerzeichen voneinander getrennt werden.

   Das Netzpräfix sollte von einem Netzadministrator angegeben werden. Das Netzpräfix muss unter Verwendung der CIDR-Notation eingegeben werden; gültige Werte sind 1 bis 24.
10. Geben Sie die Details der VADP-Konfiguration, einschließlich der IP-Adresse der IBM Spectrum Protect Plus-Appliance, an.

    Bei ESXi Server 5.5 wird diese Eingabeaufforderung angezeigt, wenn für die OVF-Implementierungsschablone der Schritt **Eigenschaften** erreicht wird.

    Bei ESXi Server 6.0 und höher wird diese Eingabeaufforderung angezeigt, wenn für die OVF-Implementierungsschablone der Schritt **Vorlage anpassen** erreicht wird.
11. Klicken Sie auf **Weiter**.
12. Überprüfen Sie Ihre Auswahlangaben für die Schablone. Klicken Sie auf **Beenden**, um den Assistenten zu verlassen und die Implementierung der OVF-Schablone zu starten. Die Implementierung kann lange dauern.
13. Nachdem die OVF-Schablone implementiert wurde, schalten Sie Ihre neu erstellte virtuelle Maschine ein. Sie können die VM über vSphere Client einschalten.

    Wichtig: Die VM muss eingeschaltet bleiben, damit auf die Anwendung IBM Spectrum Protect Plus zugegriffen werden kann.
14. Notieren Sie die IP-Adresse der neu erstellten VM.

    Die IP-Adresse ist erforderlich, um auf den vSnap-Server zugreifen und diesen registrieren zu können. Sie können die IP-Adresse in vSphere Client finden, indem Sie auf die VM klicken und die Registerkarte **Zusammenfassung** überprüfen.

Nächste Schritte

Führen Sie nach der Installation des vSnap-Servers die folgende Aktion aus:

Aktion	Vorgehensweise
Fügen Sie den vSnap-Server IBM Spectrum Protect Plus hinzu und konfigurieren Sie die vSnap-Umgebung.	Siehe „vSnap-Server verwalten” auf Seite 59.
Konfigurieren Sie die VADP-Umgebung.	Siehe „Optionen für VADP-Proxys definieren” auf Seite 114.

Virtuellen vSnap-Server in einer Hyper-V-Umgebung installieren

Um einen vSnap-Server in einer Hyper-V-Umgebung zu installieren, importieren Sie eine Hyper-V-Schablone. Damit wird eine virtuelle Appliance erstellt, die den vSnap-Server auf einer virtuellen Hyper-V-Maschine enthält.

Vorbereitende Schritte

Für alle Hyper-V-Server, einschließlich Clusterknoten, muss der Microsoft-iSCSI-Initiator-Dienst in der Liste "Dienste" aktiv sein. Setzen Sie den Dienst auf "Automatisch", sodass er verfügbar ist, wenn die Maschine erneut gestartet wird.

Vorgehensweise

1. Laden Sie die vSnap-Installationsdatei `CC1QFML.exe` von Passport Advantage Online herunter. Informationen zum Herunterladen von Dateien finden Sie in Technote 879861.
2. Kopieren Sie die Installationsdatei auf Ihren Hyper-V-Server.
3. Starten Sie das Installationsprogramm und führen Sie die Installationsschritte aus.
4. Öffnen Sie Hyper-V-Manager und wählen Sie den erforderlichen Server aus. Informationen zu Hyper-V-Systemanforderungen finden Sie in Systemanforderungen für Hyper-V unter Windows Server.
5. Klicken Sie in Hyper-V-Manager im Menü **Aktionen** auf **Virtuellen Computer importieren** und dann auf **Weiter**. Das Dialogfenster **Ordner suchen** wird geöffnet.
6. Navigieren Sie zu der Position des Ordners "Virtuelle Computer" innerhalb des dekomprimierten vSnap-Ordners. Klicken Sie auf **Weiter**. Das Dialogfenster **Virtuellen Computer auswählen** wird geöffnet.
7. Wählen Sie "vSnap" aus und klicken Sie dann auf **Weiter**. Das Dialogfenster **Importtyp auswählen** wird geöffnet.
8. Wählen Sie den folgenden Importtyp aus: **Virtuellen Computer direkt registrieren**. Klicken Sie auf **Weiter**.
9. Wenn das Dialogfenster "Netzwerk verbinden" geöffnet wird, geben Sie den zu verwendenden virtuellen Switch an und klicken Sie dann auf **Weiter**. Das Dialogfenster "Fertigstellen des Import-Assistenten" wird geöffnet.
10. Überprüfen Sie die Beschreibung und klicken Sie dann auf **Fertig stellen**, um den Importprozess abzuschließen und den Assistenten **Virtuellen Computer importieren** zu schließen. Die virtuelle Maschine wird importiert.
11. Klicken Sie mit der rechten Maustaste auf die neu implementierte VM und klicken Sie dann auf **Einstellungen**.
12. Wählen Sie unter dem Abschnitt "IDE-Controller 0" **Festplatte** aus.
13. Klicken Sie auf **Bearbeiten** und dann auf **Weiter**.
14. Wählen Sie in der Anzeige **Aktion auswählen Konvertieren** aus und klicken Sie dann auf **Weiter**.
15. Wählen Sie für das Datenträgerformat **VHDX** aus.
16. Wählen Sie für den Datenträgertyp **Feste Größe** aus.
17. Ordnen Sie für die Option "Datenträger konfigurieren" dem Datenträger einen neuen Namen und wahlweise eine neue Position zu.
18. Überprüfen Sie die Beschreibung und klicken Sie dann auf **Fertig stellen**, um die Konvertierung abzuschließen.
19. Klicken Sie auf **Durchsuchen**, um nach der neu erstellten VHDX zu suchen, und wählen Sie diese dann aus.
20. Wiederholen Sie die Schritte 12 bis 18 für jeden Datenträger unter dem Abschnitt "SCSI-Controller".
21. Schalten Sie die VM über **Hyper-V-Manager** ein. Wählen Sie auf Anforderung die Option zum Starten des Kernels im Wiederherstellungsmodus aus.
22. Ermitteln Sie mithilfe von Hyper-V-Manager die IP-Adresse der neuen virtuellen Maschine, sofern die Adresse automatisch zugeordnet wurde. Informationen zum Zuordnen einer statischen IP-Adresse zu der virtuellen Maschine mithilfe von NetworkManager Text User Interface finden Sie im folgenden Abschnitt.
23. Wenn die Adresse der neuen VM automatisch zugeordnet wird, verwenden Sie Hyper-V-Manager zum Ermitteln der IP-Adresse. Um einer VM eine statische IP-Adresse zuzuordnen, verwenden Sie das Tool NetworkManager Text User Interface (nmtui). Anweisungen finden Sie in „Statische IP-Adresse zuordnen” auf Seite 50.

Nächste Schritte
Führen Sie nach der Installation des vSnap-Servers die folgende Aktion aus:

Aktion	Vorgehensweise
Fügen Sie den vSnap-Server IBM Spectrum Protect Plus hinzu und konfigurieren Sie die vSnap-Umgebung.	Siehe „vSnap-Server verwalten” auf Seite 59.

vSnap-Server verwalten

Um Sicherungs- und Zurückschreibungsjobs zu aktivieren, sind mindestens eine virtuelle IBM Spectrum Protect Plus-Appliance und mindestens ein vSnap-Server erforderlich. Der vSnap-Server kann sich auf der IBM Spectrum Protect Plus-Appliance oder auf einer eigenen Appliance befinden, oder es kann sich um eine physische vSnap-Installation handeln. Jede vSnap-Serverposition muss hinzugefügt werden, damit sie von IBM Spectrum Protect Plus erkannt wird.

vSnap-Server als Sicherungsspeicherprovider hinzufügen

Der integrierte vSnap-Server wird in IBM Spectrum Protect Plus registriert, wenn die Appliance implementiert wird. Sie müssen alle zusätzlichen Server hinzufügen, die auf virtuellen oder physischen Appliances installiert sind, damit sie von IBM Spectrum Protect Plus erkannt werden.

Vorbereitende Schritte

Nachdem Sie einen vSnap-Server als Sicherungsspeicherprovider hinzugefügt haben, müssen Sie möglicherweise bestimmte Aspekte von vSnap konfigurieren und verwalten, wie z. B. die Netzkonfiguration oder die Speicherpoolverwaltung. Weitere Informationen finden Sie in „Referenz für vSnap-Serververwaltung” auf Seite 64.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen vSnap-Server als Sicherungsspeichereinheit hinzuzufügen:

1. Melden Sie sich bei der vSnap-Serverkonsole mit der Benutzer-ID `serveradmin` an. Das Anfangskennwort ist `sppDP758`.

   Sie werden bei der ersten Anmeldung aufgefordert, dieses Kennwort zu ändern.
2. Führen Sie den Befehl **`vsnap user create`** aus, um einen Benutzernamen und ein Kennwort für den vSnap-Server zu erstellen.
3. Starten Sie die IBM Spectrum Protect Plus-Benutzerschnittstelle, indem Sie den Hostnamen oder die IP-Adresse der virtuellen Maschine eingeben, auf der IBM Spectrum Protect Plus in einem unterstützten Browser implementiert ist.
4. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Sicherungsspeicher** > **Platte**.
5. Klicken Sie auf **Plattenspeicher hinzufügen**.
6. Füllen Sie die Felder im Fenster **Speichereigenschaften** aus:

   Hostname/IP
   Geben Sie die auflösbare IP-Adresse oder den Hostnamen des Sicherungsspeichers ein.

   Site
   Wählen Sie eine Site für den Sicherungsspeicher aus. Verfügbare Optionen sind **Primär**, **Sekundär** oder **Neue Site hinzufügen**. Sind mehrere primäre, sekundäre oder benutzerdefinierte Sites für IBM Spectrum Protect Plus verfügbar, wird zunächst die Site mit dem größten verfügbaren Speicher verwendet.

   Benutzername
   Geben Sie den Benutzernamen für den vSnap-Server ein, der in Schritt „2” auf Seite 59 erstellt wurde.

Kennwort
Geben Sie das Kennwort für den Benutzer ein.

7. Klicken Sie auf **Speichern**.
   IBM Spectrum Protect Plus bestätigt eine Netzverbindung und fügt die Sicherungsspeichereinheit zur Datenbank hinzu.

Nächste Schritte
Führen Sie die folgenden Aktionen aus, nachdem Sie einen Sicherungsspeicherprovider hinzugefügt haben:

Aktion	Vorgehensweise
Initialisieren Sie den vSnap-Server.	Siehe „vSnap-Server initialisieren” auf Seite 60.
Erweitern Sie den vSnap-Speicherpool.	Siehe „vSnap-Speicherpool erweitern” auf Seite 62.
Falls erforderlich, konfigurieren und verwalten Sie bestimmte Aspekte von vSnap, wie z. B. die Netzkonfiguration oder die Speicherpoolverwaltung.	„Referenz für vSnap-Serververwaltung” auf Seite 64

Zugehörige Tasks
„IBM Spectrum Protect Plus starten” auf Seite 73
Starten Sie IBM Spectrum Protect Plus, um die Anwendung und ihre Funktionen verwenden zu können.

Einstellungen für einen vSnap-Server editieren
Sie können die Konfigurationseinstellungen für einen vSnap-Server editieren, um Änderungen in Ihrer IBM Spectrum Protect Plus-Umgebung widerzuspiegeln.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Einstellungen für einen vSnap-Server zu editieren:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Sicherungsspeicher** > **Platte**.
2. Klicken Sie auf das Symbol für Editieren , das einem vSnap-Server zugeordnet ist.
   Das Fenster **Speicher editieren** wird angezeigt.
3. Überarbeiten Sie die vSnap-Servereinstellungen und klicken Sie dann auf **Speichern**.

vSnap-Server löschen
Sie können einen vSnap-Server löschen, der in Ihrer IBM Spectrum Protect Plus-Umgebung nicht mehr verwendet wird, löschen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen vSnap-Server zu löschen:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Sicherungsspeicher** > **Platte**.
2. Klicken Sie auf das Symbol für Löschen , das einem vSnap-Server zugeordnet ist.
3. Klicken Sie auf **Ja**, um den Server aus IBM Spectrum Protect Plus zu löschen.

vSnap-Server initialisieren

Beim Initialisierungsprozess wird ein neuer vSnap-Server für die Verwendung vorbereitet, indem Softwarekomponenten geladen und konfiguriert werden und die interne Konfiguration initialisiert wird. Dies ist ein einmaliger Prozess, der nur für Neuinstallationen ausgeführt werden muss.

Informationen zu diesem Vorgang

Als Teil des Initialisierungsprozesses erstellt vSnap einen Speicherpool, indem alle verfügbaren nicht verwendeten Platten im System verwendet werden. Die OVA-basierten Implementierungen von vSnap enthalten jeweils eine nicht verwendete virtuelle Platte mit standardmäßig 100 GB, die zum Erstellen des Pools verwendet wird.

Werden keine nicht verwendeten Platten gefunden, wird der Initialisierungsprozess ohne Erstellung eines Pools ausgeführt.

Informationen zum Erweitern, Erstellen und Verwalten von Speicherpools finden Sie in „Speichermanagement" auf Seite 65.

Sie können die IBM Spectrum Protect Plus-Benutzerschnittstelle oder die vSnap-Serverkonsole verwenden, um vSnap-Server zu initialisieren.

Für Server, die in einer virtuellen Umgebung implementiert werden, bietet die Benutzerschnittstelle eine einfache Methode, um die Initialisierungsoperation auszuführen.

Für Server, die in einer physischen Umgebung implementiert werden, bietet die vSnap-Serverkonsole mehr Optionen für die Initialisierung des Servers, einschließlich der Möglichkeit, einen Speicherpool mithilfe von erweiterten Redundanzoptionen und einer bestimmten Liste von Platten zu erstellen.

Einfache Initialisierung ausführen

Um einen vSnap-Server für die Verwendung vorzubereiten, müssen Sie den vSnap-Server initialisieren. Verwenden Sie IBM Spectrum Protect Plus, um einen vSnap-Server zu initialisieren, der in einer virtuellen Umgebung implementiert wird.

Informationen zu diesem Vorgang

Für die Installation des integrierten vSnap-Servers, der als Teil einer IBM Spectrum Protect Plus-Installation registriert wird, werden Sie zum Starten des Initialisierungsprozesses aufgefordert, wenn Sie sich zum ersten Mal bei der Benutzerschnittstelle anmelden. Es sind keine weiteren Schritte erforderlich.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen vSnap-Server mithilfe der IBM Spectrum Protect Plus-Benutzerschnittstelle zu initialisieren:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Sicherungsspeicher** > **Platte**.
2. Wählen Sie im Menü **Aktionen**, das dem Server zugeordnet ist, die Initialisierungsmethode aus:

   Mit Verschlüsselung initialisieren
   Aktivieren Sie die Verschlüsselung von Sicherungsdaten auf dem vSnap-Server.

   Initialisieren
   Initialisieren Sie den vSnap-Server ohne aktivierter Verschlüsselung.

   Der Initialisierungsprozess wird im Hintergrund ausgeführt und erfordert keine weitere Benutzerinteraktion. Die Ausführung des Prozesses kann 5 bis 10 Minuten dauern.

Erweiterte Initialisierung ausführen

Verwenden Sie die vSnap-Serverkonsole, um einen vSnap-Server zu initialisieren, der in einer physischen Umgebung implementiert wird. Die Initialisierung mithilfe der vSnap-Serverkonsole bietet mehr Optionen für die Initialisierung des Servers, einschließlich der Möglichkeit, einen Speicherpool mithilfe von erweiterten Redundanzoptionen und einer bestimmten Liste von Platten zu erstellen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen vSnap-Server mithilfe der vSnap-Serverkonsole zu initialisieren:

1. Melden Sie sich bei der vSnap-Serverkonsole mit der Benutzer-ID `serveradmin` an. Das Anfangskennwort ist `sppDP758`.

Sie können auch eine Benutzer-ID mit vSnap-Administratorberechtigungen verwenden, die mithilfe des Befehls **vsnap user create** erstellt wird. Weitere Informationen zur Verwendung von Konsolenbefehlen finden Sie in „Referenz für vSnap-Serververwaltung” auf Seite 64.

2. Führen Sie den Befehl **vsnap system init --skip_pool** aus. Der Befehl erfordert keine weitere Interaktion und führt alle Initialisierungstasks mit Ausnahme der Erstellung eines Speicherpools aus. Die Ausführung des Prozesses kann 5 bis 10 Minuten dauern.

Nächste Schritte

Führen Sie die folgende Aktion aus, nachdem Sie die Initialisierung beendet haben:

Aktion	Vorgehensweise
Erstellen Sie einen Speicherpool.	Siehe „Speichermanagement” auf Seite 65.

vSnap-Speicheroptionen festlegen

Sie können weitere speicherbezogene Optionen für einen vSnap-Server festlegen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Optionen für einen vSnap-Server festzulegen:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Sicherungsspeicher** > **Platte**.
2. Klicken Sie auf das Symbol für Verwalten , das dem vSnap-Server zugeordnet ist, und erweitern Sie dann den Abschnitt **Speicheroptionen**. Legen Sie die Speicheroptionen fest.

   Komprimierung aktivieren

   Falls aktiviert, wird jeder eingehende Datenblock unter Verwendung eines Komprimierungsalgorithmus komprimiert, bevor er in den Speicherpool geschrieben wird. Für die Komprimierung werden relativ wenige zusätzliche CPU-Ressourcen verbraucht.

   Deduplizierung aktivieren

   Falls aktiviert, wird jeder eingehende Datenblock hashverschlüsselt und mit vorhandenen Blöcken im Speicherpool verglichen. Wenn die Komprimierung aktiviert ist, werden die Daten nach der Komprimierung verglichen. Doppelte Blöcke werden nicht in den Pool geschrieben, sondern übersprungen. Die Deduplizierung ist standardmäßig inaktiviert, da sie sehr viele Speicherressourcen (proportional zum Datenvolumen im Pool) verbraucht, um die Deduplizierungstabelle von Blockhashes zu verwalten.

   Modus für synchrones Schreiben

   Die Inaktivierung synchroner Schreibvorgänge kann zu einem Datenverlust und zur schleichenden Beschädigung von Sicherungsdaten führen, wenn der Speicherserver während eines Sicherungsjobs abrupt heruntergefahren oder neu gestartet wird. Inaktivieren Sie diese Option nur, wenn sich der Speicherserver in einer stabilen Umgebung befindet, die ausreichend vor Hardwarefehlern und Stromausfall geschützt ist.

   Verschlüsselung aktiviert

   Mit dieser Option wird der Verschlüsselungsstatus des vSnap-Servers angezeigt. Die Verschlüsselung kann nur während der vSnap-Initialisierung aktiviert werden. Diese Option dient nur zu Informationszwecken.
3. Klicken Sie auf **Speichern**.

vSnap-Speicherpool erweitern

Wenn IBM Spectrum Protect Plus zurückmeldet, dass ein vSnap-Server seine Speicherkapazität fast erreicht hat, muss der vSnap-Speicherpool erweitert werden. Um einen vSnap-Speicherpool zu erweitern, müssen Sie zuerst virtuelle oder physische Platten auf dem vSnap-Server hinzufügen, indem Sie entweder der virtuellen vSnap-Maschine virtuelle Platten hinzufügen oder dem physischen vSnap-Server physische Platten hinzufügen. Die vSphere-Dokumentation enthält Informationen zum Erstellen zusätzlicher virtueller Platten.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen vSnap-Speicherpool zu erweitern:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Sicherungsspeicher** > **Platte**.
2. Wählen Sie **Aktionen** > **Erneut überprüfen** für den vSnap-Server aus, der erneut überprüft werden soll.
3. Klicken Sie auf das Symbol für Verwalten , das dem vSnap-Server zugeordnet ist, und erweitern Sie dann den Abschnitt **Neue Platten zum Sicherungsspeicher hinzufügen**.
4. Fügen Sie die ausgewählten Platten hinzu und speichern Sie die Platten. Der vSnap-Pool wird um die Größe der hinzugefügten Platten erweitert.

Replikationspartnerschaft für einen vSnap-Server erstellen

Mithilfe der Sicherungsspeicherreplikation können Sie Daten asynchron von einem vSnap-Server auf einem anderen vSnap-Server sichern.

Vorbereitende Schritte

Alle vSnap-Server müssen denselben Versionsstand haben, damit die Replikation funktioniert. Die Replikation zwischen unterschiedlichen Versionen wird nicht unterstützt.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Replikationspartnerschaft zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Sicherungsspeicher** > **Platte**.
2. Klicken Sie auf das Symbol für Verwalten , das dem vSnap-Server zugeordnet ist, dem eine Replikationspartnerschaft hinzugefügt werden soll, und erweitern Sie dann den Abschnitt **Speicherpartner konfigurieren**.
3. Klicken Sie auf das Symbol für Hinzufügen .
4. Wählen Sie in der Liste **Partner auswählen** einen vSnap-Server aus, mit dem eine Replikationspartnerschaft erstellt werden soll.
5. Klicken Sie auf **Partner hinzufügen**.

Nächste Schritte

Führen Sie nach dem Erstellen einer Replikationspartnerschaft die folgende Aktion aus, um die Replikation zu aktivieren:

Aktion	Vorgehensweise
Wählen Sie die Option **Sicherungsspeicherreplikation** in der SLA-Richtlinie aus, die dem Sicherungsjob zugeordnet ist.	Siehe „SLA-Richtlinie erstellen” auf Seite 93.

Auslagerungsdurchsatzrate ändern

Ändern Sie den Durchsatz für Replikations- und Auslagerungsoperationen an Ihrer Site, sodass Sie die Netzaktivität in einem definierten Zeitplan verwalten können.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Site**, um das Fenster **Siteeigenschaften** zu öffnen.
2. Klicken Sie auf das Symbol für Editieren , das der Site zugeordnet ist, für die der Durchsatz geändert werden soll.
3. Klicken Sie auf **Drosselung aktivieren**.

Die Rate des Durchsatzes wird in MB/s angezeigt.

4. Passen Sie den Durchsatz an:
   - Ändern Sie die Durchsatzrate mit den Aufwärts- und Abwärtspfeilen.
   - Ändern Sie den Datenwert. Die Auswahlmöglichkeiten umfassen Byte/s, KB/s, MB/s und GB/s.

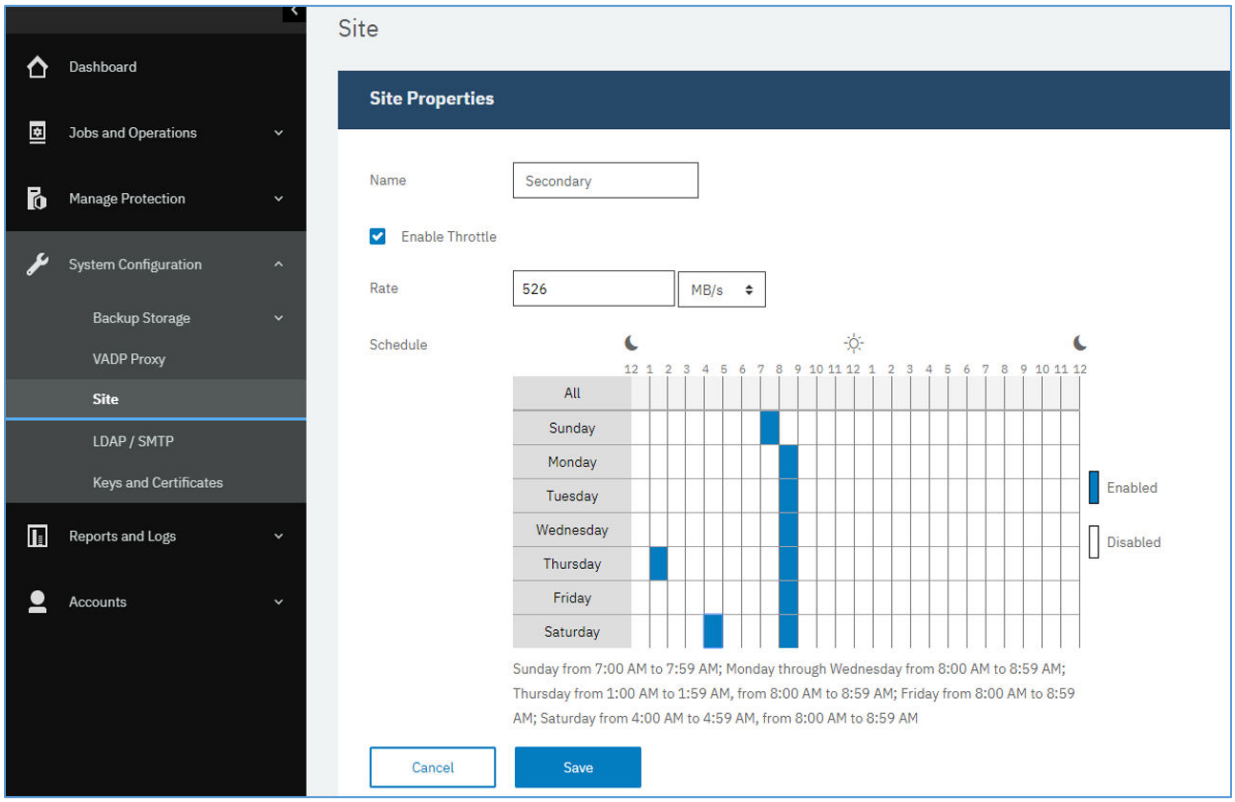


Abbildung 4. Verschiedene Drosselungen für verschiedene Zeitpunkte zur Verbesserung des Durchsatzes aktivieren

5. Wählen Sie in der Tabelle mit der Wochenübersicht Zeiten für den geänderten Durchsatz aus oder geben Sie einen Tag und eine Uhrzeit für die geänderte Rate an.

   Anmerkung: Um den Inhalt eines Zeitfensters zu löschen, klicken Sie auf das Zeitfenster. Die geplanten Auswahlangaben werden unter der Tabelle mit dem Zeitplan aufgelistet.
6. Klicken Sie auf **Speichern**, um die Änderungen festzuschreiben und die Anzeige zu schließen.

Referenz für vSnap-Serververwaltung

Nach der Installation, Registrierung und Initialisierung des vSnap-Servers verwaltet IBM Spectrum Protect Plus dessen Verwendung als Sicherungsziel automatisch. Datenträger und Momentaufnahmen werden gemäß den in IBM Spectrum Protect Plus definierten SLA-Richtlinien automatisch erstellt und verwaltet.

Sie müssen aber möglicherweise dennoch bestimmte Aspekte von vSnap konfigurieren und verwalten, wie z. B. die Netzkonfiguration oder die Speicherpoolverwaltung.

vSnap über die Befehlszeilenschnittstelle verwalten

Die vSnap-Befehlszeilenschnittstelle ist die primäre Methode zur Verwaltung von vSnap. Für den Zugriff auf die Befehlszeilenschnittstelle führen Sie den Befehl **vsnap** aus. Der Befehl kann von der Benutzer-ID `serveradmin` oder von einem beliebigen anderen Betriebssystembenutzer mit vSnap-Administratorberechtigungen aufgerufen werden. Führen Sie den Befehl **`vsnap user create`** aus, um zusätzliche Be-

triebssystembenutzer zu erstellen, die über diese Berechtigungen verfügen. Das Anfangskennwort von `serveradmin` ist sppDP758.

Dem Benutzer `serveradmin` sind standardmäßig keine sudo-Berechtigungen zugeordnet. Wenn dem Benutzer `serveradmin` sudo-Berechtigungen zugeordnet werden sollen, melden Sie sich bei der Befehlszeilenschnittstelle des vSnap-Servers an und geben Sie den folgenden Befehl ein:

```
echo "serveradmin ALL=(ALL) NOPASSWD: ALL" >/etc/sudoers.d/serveradmin
```

Die Befehlszeilenschnittstelle besteht aus mehreren Befehlen und Unterbefehlen, die verschiedene Aspekte des Systems verwalten. Details zur Verwendung dieser Befehle finden Sie in „Speichermanagement” auf Seite 65 und in „Netzmanagement” auf Seite 68. Sie können auch das Flag **`--help`** an jeden Befehl oder Unterbefehl anfügen, um Hilfe zur Syntax aufzurufen. Zum Beispiel **`vsnap --help`** oder **`vsnap pool create --help`**.

vSnap über die IBM Spectrum Protect Plus-Benutzerschnittstelle verwalten

Einige der häufigsten Operationen können auch über die IBM Spectrum Protect Plus-Benutzerschnittstelle ausgeführt werden. Melden Sie sich bei der Benutzerschnittstelle an und klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Sicherungsspeicher** > **Platte**. Klicken Sie auf das Symbol für Verwalten  eines vSnap-Servers, um diesen zu verwalten.

Zugehörige Tasks

„vSnap-Server installieren” auf Seite 55
Wenn Sie eine IBM Spectrum Protect Plus-Appliance implementieren, wird automatisch ein vSnap-Server installiert. Dieser Server ist das primäre Sicherungsziel. In umfangreicheren Unternehmensumgebungen sind unter Umständen weitere vSnap-Server erforderlich.

„vSnap-Server verwalten” auf Seite 59
Um Sicherungs- und Zurückschreibungsjobs zu aktivieren, sind mindestens eine virtuelle IBM Spectrum Protect Plus-Appliance und mindestens ein vSnap-Server erforderlich. Der vSnap-Server kann sich auf der IBM Spectrum Protect Plus-Appliance oder auf einer eigenen Appliance befinden, oder es kann sich um eine physische vSnap-Installation handeln. Jede vSnap-Serverposition muss hinzugefügt werden, damit sie von IBM Spectrum Protect Plus erkannt wird.

Speichermanagement

Sie können Speicherpools für einen vSnap-Server konfigurieren und verwalten.

Platten verwalten

vSnap erstellt Speicherpools mithilfe von Platten, die dem vSnap-Server bereitgestellt werden. Bei virtuellen Implementierungen können die Platten RDM- oder virtuelle Platten sein, die aus Datenspeichern in einem beliebigen Sicherungsspeicher bereitgestellt werden. Bei physischen Implementierungen können die Platten lokale Platten oder Platten mit SAN-Speicheranschluss an den physischen Server sein. Für die lokalen Platten ist möglicherweise bereits externe Redundanz über einen RAID-Hardware-Controller aktiviert. Ist dies jedoch nicht der Fall, kann vSnap auch RAID-basierte Speicherpools für interne Redundanz erstellen.

An vSnap-Server angeschlossene Platten müssen Platten mit Thick Provisioning sein. Bei Platten mit Thin Provisioning hat der vSnap-Server keine präzise Sicht des freien Speicherbereichs im Speicherpool, was zu einem Datenverlust führen kann, wenn im zugrunde liegenden Datenspeicher kein Speicherbereich mehr verfügbar ist.

Wurde vSnap im Rahmen einer virtuellen Appliance implementiert, ist bereits eine virtuelle 100-GB-Startplatte enthalten, die zur Erstellung eines Pools verwendet werden kann. Sie können weitere Platten vor oder nach der Erstellung eines Pools hinzufügen und dementsprechend zur Erstellung eines größeren Pools oder zur Erweiterung eines vorhandenen Pools verwenden. Wenn in Jobprotokollen angezeigt wird, dass ein vSnap-Server seine Speicherkapazität bald ausgeschöpft hat, können dem vSnap-Pool zusätzliche Platten hinzugefügt werden. Alternativ wird durch die Erstellung neuer SLA-Richtlinien die Verwendung eines alternativen vSnap-Servers bei Sicherungen erzwungen.

Der Schutz vor einer Beschädigung, die dadurch verursacht wird, dass ein VMware-Datenspeicher auf einem vSnap-Server seine Kapazitätsgrenze erreicht, ist unbedingt notwendig. Erstellen Sie eine stabile Umgebung für virtuelle vSnap-Server, die keine RAID-Konfigurationen verwenden, indem Sie VMDKs mit Thick Provisioning einsetzen. Eine Replikation auf externe vSnap-Server bietet weiteren Schutz.

Ein vSnap-Server wird inaktiviert, wenn in einer nicht redundanten RAID-Konfiguration der vSnap-Pool oder eine vSnap-Platte gelöscht wird. Alle Daten auf dem vSnap-Server gehen verloren. Wird Ihr vSnap-Server inaktiviert, müssen Sie seine Registrierung mithilfe der IBM Spectrum Protect Plus-Schnittstelle zurücknehmen und anschließend den Verwaltungsjob ausführen. Nach Beendigung des Verwaltungsjobs kann der vSnap-Server wieder registriert werden.

Verschlüsselung verwalten

Wählen Sie **Mit aktivierter Verschlüsselung initialisieren** bei der Initialisierung des Servers aus, um die Verschlüsselung von Sicherungsdaten auf einem vSnap-Server zu aktivieren. Die Verschlüsselungseinstellungen können nach der Initialisierung des Servers und nach der Erstellung eines Pools nicht geändert werden. Alle Platten eines vSnap-Pools verwenden dieselbe Verschlüsselungsschlüsseldatei, die nach der Poolerstellung generiert wird. Die Daten werden verschlüsselt, wenn sie auf dem vSnap-Server ruhen.

Bei der vSnap-Verschlüsselung wird der folgende Algorithmus verwendet:

Verschlüsselungsname
Advanced Encryption Standard (AES)

Verschlüsselungsmodus
xts-plain64

Schlüssel
256 Bit

LUKS-Header-Hashing (Linux Unified Key Setup)
SHA-256

Verschlüsselungsschlüssel verwalten

Die nach der Poolerstellung generierten Verschlüsselungsschlüsseldateien für Platten werden im Verzeichnis '/etc/vsnap/keys/' auf jedem vSnap-Server gespeichert. Sichern Sie die Schlüsseldateien zum Zweck der Wiederherstellung nach einem Katastrophenfall manuell außerhalb des vSnap-Servers. Geben Sie nach der Erstellung eines Pools die folgenden Befehle als Benutzer 'serveradmin' ein, um die Dateien an eine temporäre Position zu kopieren und anschließend an eine gewünschte, sichere Sicherungsposition außerhalb des vSnap-Hosts zu kopieren.

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

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

Platten erkennen

Wenn Sie einem vSnap-Server Platten hinzufügen, verwenden Sie die Befehlszeile oder die IBM Spectrum Protect Plus-Benutzerschnittstelle, um die neu angeschlossenen Platten zu erkennen.

Befehlszeile: Führen Sie den Befehl **`vsnap disk rescan`** aus.

Benutzerschnittstelle: Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Sicherungsspeicher** > **Platte** und dann auf das Menü **Aktionen** neben dem betreffenden vSnap-Server und wählen Sie **Erneut überprüfen** aus.

Platten anzeigen

Führen Sie den Befehl **vsnap disk show** aus, um alle Platten aufzulisten, die sich im vSnap-System befinden.

In der Spalte USED AS der Ausgabe wird angezeigt, ob die jeweilige Platte im Gebrauch ist. Jede nicht formatierte und nicht partitionierte Platte wird als nicht verwendet gekennzeichnet. Andernfalls werden die Platten als durch die Partitionstabelle oder das Dateisystem, die bzw. das auf ihnen erkannt wird, verwendet gekennzeichnet.

Nur Platten, die als nicht verwendet gekennzeichnet sind, können zum Erstellen eines Speicherpools verwendet oder einem Speicherpool hinzugefügt werden. Wird eine Platte, die einem Speicherpool hinzugefügt werden soll, von vSnap nicht als nicht verwendet erkannt, kann dies daran liegen, dass sie zuvor schon einmal verwendet wurde und demzufolge Reste einer älteren Partitionstabelle oder eines älteren Dateisystems enthält. Eine Korrektur dieses Umstands ist mit Systembefehlen wie **parted** oder **dd** zur Bereinigung der Plattenpartitionstabelle möglich.

Speicherpoolinformationen anzeigen

Führen Sie den Befehl **vsnap pool show** aus, um Informationen zu jedem Speicherpool anzuzeigen.

Speicherpool erstellen

Wenn Sie die in „Einfache Initialisierung ausführen" auf Seite 61 beschriebene einfache Initialisierungsprozedur ausgeführt haben, wurde ein Speicherpool automatisch erstellt und die Informationen in diesem Abschnitt können übersprungen werden.

Geben Sie den Befehl **vsnap pool create** ein, um eine erweiterte Initialisierung zur manuellen Erstellung eines Speicherpools auszuführen. Bevor Sie den Befehl ausführen, müssen Sie sicherstellen, dass mindestens eine nicht verwendete Platte verfügbar ist (siehe Beschreibung in „Platten anzeigen" auf Seite 67). Um Informationen zu den verfügbaren Optionen aufzurufen, fügen Sie das Flag **--help** an einen beliebigen Befehl oder Unterbefehl an.

Geben Sie einen benutzerfreundlichen Anzeigename für den Pool und eine Liste an, die mindestens eine Platte enthält. Werden keine Platten angegeben, werden alle nicht verwendeten Platten verwendet. Sie können die Aktivierung der Komprimierung und der Deduplizierung für den Pool während der Erstellung auswählen. Sie können die Einstellungen der Komprimierung und der Deduplizierung auch später mit dem Befehl **vsnap pool update** aktualisieren.

Der während der Erstellung des Speicherpools angegebene Pooltyp legt die Redundanz des Pools fest:

raid0
: Dies ist die Standardoption, wenn kein Pooltyp angegeben wird. In diesem Fall setzt vSnap voraus, dass Ihre Platten über externe Redundanz verfügen, wenn Sie z. B. virtuelle Platten in einem Datenspeicher verwenden, der durch redundanten Speicher gesichert ist. In diesem Fall verfügt der Speicherpool über keine interne Redundanz.

  Eine Platte, die einem Pool des Typs raid0 hinzugefügt wurde, kann nicht entfernt werden. Wenn die Verbindung der Platte unterbrochen wird, hat dies zur Folge, dass der Pool nicht verfügbar wird, was nur durch Löschen und Neuerstellen des Pools behoben werden kann.

raid5
: Wenn Sie diese Option auswählen, umfasst der Pool mindestens eine RAID5-Gruppe, wobei jede Gruppe aus mindestens drei Platten besteht. Die Anzahl der RAID5-Gruppen und die Anzahl der Platten in jeder Gruppe ist von der Gesamtzahl der Platten abhängig, die Sie während der Poolerstellung angeben. Auf der Grundlage der Anzahl verfügbarer Platten wählt vSnap Werte, die die Gesamtkapazität maximieren und gleichzeitig eine optimale Redundanz notwendiger Metadaten sicherstellen.

raid6
: Wenn Sie diese Option auswählen, umfasst der Pool mindestens eine RAID6-Gruppe, wobei jede Gruppe aus mindestens vier Platten besteht. Die Anzahl der RAID6-Gruppen und die Anzahl der Platten in jeder Gruppe ist von der Gesamtzahl der Platten abhängig, die Sie während der Poolerstellung angeben. Auf der Grundlage der Anzahl verfügbarer Platten wählt vSnap Werte, die die Gesamtkapazität maximieren und gleichzeitig eine optimale Redundanz notwendiger Metadaten sicherstellen.

Speicherpool erweitern

Bevor Sie einen Pool erweitern, müssen Sie sicherstellen, dass mindestens eine nicht verwendete Platte verfügbar ist (siehe Beschreibung in „Platten anzeigen” auf Seite 67).

Verwenden Sie für die Erweiterung eines Speicherpools die Befehlszeile oder die IBM Spectrum Protect Plus-Benutzerschnittstelle.

Befehlszeile: Führen Sie den Befehl **`vsnap pool expand`** aus. Um Informationen zu den verfügbaren Optionen aufzurufen, fügen Sie das Flag **`--help`** an einen beliebigen Befehl oder Unterbefehl an.

Benutzerschnittstelle: Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Sicherungsspeicher** > **Platte**. Klicken Sie auf das Symbol für Verwalten  eines vSnap-Servers, um diesen zu verwalten, und blenden Sie anschließend die Registerkarte **Neue Platten hinzufügen** ein. Auf der Registerkarte werden alle nicht verwendeten Platten angezeigt, die auf dem System erkannt werden. Wählen Sie mindestens eine Platte aus und klicken Sie auf **Speichern**, um sie dem Speicherpool hinzuzufügen.

Netzmanagement

Sie können Netzservices für einen vSnap-Server konfigurieren und verwalten.

Netzschnittstelleninformationen anzeigen

Führen Sie den Befehl **`vsnap network show`** aus, um die Netzschnittstellen und die jeweils zugeordneten Services aufzulisten.

Standardmäßig sind die folgenden vSnap-Services für alle Netzschnittstellen verfügbar:

mgmt
: Dieser Service wird für Managementdatenverkehr zwischen IBM Spectrum Protect Plus und vSnap verwendet.

nfs
: Dieser Service wird für Datenverkehr bei der Datensicherung mithilfe von NFS verwendet.

iscsi
: Dieser Service wird für Datenverkehr bei der Datensicherung mithilfe von iSCSI verwendet.

smb
: Dieser Service wird für Datenverkehr bei der Datensicherung mithilfe von SMB/CIFS verwendet.

repl
: Dieser Service wird für Datenverkehr zwischen vSnap-Servern während der Replikation verwendet.

Zugeordnete Netzschnittstellenservices ändern

Führen Sie den Befehl **`vsnap network update`** aus, um Services zu ändern, die einer Schnittstelle zugeordnet sind. Zum Beispiel, wenn Sie eine dedizierte Schnittstelle für Datenverkehr zur Verbesserung der Leistung verwenden.

Folgende Optionen sind erforderlich:

`--id <ID>`
: Geben Sie die ID der zu aktualisierenden Schnittstelle ein.

`--services <Services>`
: Geben Sie `all` oder eine durch Kommas getrennte Liste der Services an, die in der Schnittstelle aktiviert werden sollen. Gültige Werte: `mgmt`, `nfs`, `smb` und `iscsi`.

Ist ein Service in mehreren Schnittstellen verfügbar, kann IBM Spectrum Protect Plus jede der Schnittstellen verwenden.

Stellen Sie sicher, dass der Service mgmt in der Schnittstelle, die für die Registrierung des vSnap-Servers in IBM Spectrum Protect Plus verwendet wurde, aktiviert bleibt.

vSnap-Server deinstallieren

Sie können einen vSnap-Server aus Ihrer IBM Spectrum Protect Plus-Umgebung entfernen.

Vorbereitende Schritte

Stellen Sie sicher, dass keine Jobs SLA-Richtlinien verwenden, die den vSnap-Server als Sicherungsposition verwenden. Um die SLA-Richtlinien anzuzeigen, die Jobs zugeordnet sind, rufen Sie die Seite **Sicherung** für den Hypervisor oder die Anwendung auf, dessen bzw. deren Sicherung geplant ist. Klicken Sie beispielsweise für VMware-Sicherungsjobs auf **Schutz verwalten** > **Hypervisoren** > **VMware**.

Vorgehensweise

1. Melden Sie sich bei der vSnap-Serverkonsole mit der Benutzer-ID `serveradmin` an. Das Anfangskennwort ist sppDP758.

   Sie können auch eine Benutzer-ID mit vSnap-Administratorberechtigungen verwenden, die mithilfe des Befehls **`vsnap user create`** erstellt wird. Weitere Informationen zur Verwendung von Konsolenbefehlen finden Sie in „Referenz für vSnap-Serververwaltung” auf Seite 64.
2. Führen Sie die folgenden Befehle aus:

   ```
   systemctl stop vsnap
   yum remove vsnap
   ```
3. Optional: Wenn nicht geplant ist, den vSnap-Server nach seiner Deinstallation erneut zu installieren, entfernen Sie die Daten und die Konfiguration, indem Sie die folgenden Befehle ausführen:

   ```
   rm -rf /etc/vsnap
   rm -rf /etc/nginx
   rm -rf /etc/uwsgi.d
   rm -f /etc/uwsgi.ini
   ```
4. Führen Sie einen Warmstart für das System durch, um sicherzustellen, dass Kernelmodule entladen werden, und heben Sie die Zuordnung der Datenplatten, die vSnap-Pooldaten enthalten, auf.

   Anmerkung: Um IBM Spectrum Protect Plus in einer Hyper-V-Umgebung zu deinstallieren, löschen Sie die SPP-Appliance aus Hyper-V und löschen Sie dann das Installationsverzeichnis.

Ergebnisse

Nach der Deinstallation eines vSnap-Servers wird die Konfiguration im Verzeichnis `/etc/vsnap` beibehalten. Die Konfiguration wird wiederverwendet, wenn der vSnap-Server erneut installiert wird. Die Konfiguration wird entfernt, wenn die optionalen Befehle zum Entfernen der Konfigurationsdaten ausgeführt wurden.

Kapitel 4. Schnelleinstieg

Damit Sie IBM Spectrum Protect Plus verwenden können, müssen Sie zunächst verschiedene Schritte ausführen; diese Schritte umfassen das Definieren der Ressourcen, die geschützt werden sollen, und das Erstellen von SLA-Richtlinien (SLA = Service-Level-Agreement), die auch als Sicherungsrichtlinien bezeichnet werden, für diese Ressourcen. In diesem Einführungsabschnitt finden Sie die grundlegenden Schritte für die Konfiguration von IBM Spectrum Protect Plus und den Einstieg zur Verwendung des Produkts zum Sichern von Daten. Andere Tasks wie die Auslagerung und Zurückschreibung von Daten werden in anderen Abschnitten der Dokumentation ausführlich erläutert.

Bevor Sie beginnen, müssen Sie sicherstellen, dass Sie die Anweisungen in den IBM Spectrum Protect Plus Blueprints ausgeführt haben, um zu bestimmen, wie Sie in Ihrer IBM Spectrum Protect Plus-Umgebung die Anzahl Komponenten festlegen sowie Komponenten erstellen und integrieren; außerdem müssen Sie sicherstellen, dass die in der „Roadmap für die Produktimplementierung” auf Seite 11 aufgelisteten Tasks ausgeführt wurden.

Wie die folgende Tabelle zeigt, werden die Erstinstallations- und -konfigurationstasks vom IBM Spectrum Protect Plus-*Infrastrukturadministrator* ausgeführt. Standardmäßig wird der Benutzeraccount `admin` für die Verwendung durch den Infrastrukturadministrator für den ersten Start der Anwendung erstellt.

Anschließend werden Sicherungs- und Zurückschreibungstasks für Hypervisoren und Datenbankanwendungen vom *Anwendungsadministrator* ausgeführt. In Ihrer Umgebung könnte jedoch ein einziger Administrator für alle Tasks verantwortlich sein.

Aktion	**Eigner**	
IBM Spectrum Protect Plus starten	Infrastrukturadministrator und Anwendungsadministrator	Der Infrastrukturadministrator führt den ersten Start der Anwendung mit dem Standardbenutzeraccount `admin` und dem Kennwort `password` aus. Der Administrator wird nach der Anmeldung zum Zurücksetzen des Benutzernamens für diesen Account aufgefordert. Der Administrator kann den Benutzernamen nicht auf `admin`, `root` oder `test` zurücksetzen. Nach dem ersten Start kann der Anwendungsadministrator die Anwendung mit diesem Benutzeraccount oder einem anderen Account, der vom Infrastrukturadministrator erstellt wird, starten.

© Copyright IBM Corp. 2017, 2019

Aktion	Eigner	
„Sites verwalten” auf Seite 74	Infrastrukturadministrator	Eine Site dient dazu, vSnap-Server auf der Basis einer physischen oder logischen Position zu gruppieren, um so ein schnelles Auffinden von Sicherungsdaten und die Interaktion mit Sicherungsdaten zu ermöglichen. Eine Site wird einem vSnap-Server zugeordnet, wenn der Server IBM Spectrum Protect Plus hinzugefügt wird. Die Standardsites haben die Namen 'Primär' und 'Sekundär'; es kann jedoch auch eine angepasste Site erstellt und beim Hinzufügen des vSnap-Servers zugeordnet werden. Überprüfen Sie, bevor Sie mit den folgenden Aktionen fortfahren, die verfügbaren Sites und bestimmen Sie, ob neue Sites hinzugefügt oder die vorhandenen geändert werden sollen.
Sicherungsrichtlinien erstellen	Infrastrukturadministrator	Sicherungsrichtlinien definieren die Parameter, die auf Sicherungsjobs angewendet werden. Diese Parameter umfassen die Häufigkeit und die Aufbewahrung von Sicherungen und die Optionen zur Replikation von Daten von einem vSnap-Server auf einen anderen und zur Auslagerung von Sicherungsdaten in sekundären Sicherungsspeicher für den längerfristigen Schutz. Sicherungsrichtlinien definieren außerdem die Zielsite für das Sichern von Daten. Eine Site kann einen oder mehrere vSnap-Server enthalten. Sicherungsrichtlinien werden in IBM Spectrum Protect Plus als SLA-Richtlinien bezeichnet.
Benutzeraccount für den Anwendungsadministrator erstellen	Infrastrukturadministrator	Benutzeraccounts legen die Ressourcen und Funktionen fest, die für den Benutzer verfügbar sind.

Aktion	Eigner	
Zu schützende Ressourcen hinzufügen	Anwendungsadministrator	Ressourcen sind Server für Hypervisoren oder Datenbankanwendungen, auf denen Daten gehostet werden, die geschützt werden sollen.
Ressourcen einer Jobdefinition hinzufügen	Anwendungsadministrator	Jobdefinitionen ordnen die Ressourcen, die geschützt werden sollen, einer oder mehreren SLA-Richtlinien zu. Die in den SLA-Richtlinien definierten Optionen und Zeitpläne werden für Sicherungsjob für die Ressourcen verwendet.
Sicherungsjob starten	Anwendungsadministrator	Sicherungsjobs werden gemäß der Definition in der SLA-Richtlinie, die der Jobdefinition zugeordnet ist, gestartet. Sie können einen Job auch manuell starten.
Bericht ausführen	Anwendungsadministrator	IBM Spectrum Protect Plus stellt eine Reihe vordefinierter Berichte bereit, die Sie mit Standardparametern ausführen oder ändern können, um angepasste Berichte zu erstellen.

IBM Spectrum Protect Plus starten

Starten Sie IBM Spectrum Protect Plus, um die Anwendung und ihre Funktionen verwenden zu können.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um IBM Spectrum Protect Plus zu starten:

1. Geben Sie in einem unterstützten Browser die folgende URL ein:

   ```
   https://Hostname
   ```

   Dabei ist *Hostname* die IP-Adresse der virtuellen Maschine, auf der die Anwendung implementiert ist. Damit wird die Verbindung zu IBM Spectrum Protect Plus hergestellt.
2. Geben Sie Ihren Benutzernamen und das Kennwort für die Anmeldung ein.

   Wenn es sich um die erste Anmeldung handelt, lautet der Standardbenutzername `admin` und das Kennwort `password`. Sie werden dazu aufgefordert, den Standardbenutzernamen und das Kennwort zurückzusetzen. Sie können den Benutzernamen nicht auf `admin`, `root` oder `test` zurücksetzen.
3. Klicken Sie auf **Anmelden**.
4. Wenn Sie sich zum ersten Mal bei IBM Spectrum Protect Plus anmelden, werden Sie zur Ausführung der folgenden Aktionen aufgefordert:
   - Ändern Sie das Kennwort für `serveradmin`. Das Anfangskennwort ist sppDP758. Der Benutzer `serveradmin` wird für den Zugriff auf die Verwaltungskonsole und die virtuelle IBM Spectrum Protect Plus-Appliance verwendet. Das Kennwort für `serveradmin` muss geändert werden, bevor auf die Verwaltungskonsole und die virtuelle IBM Spectrum Protect Plus-Appliance zugegriffen wird.
   - Starten Sie den Initialisierungsprozess für den integrierten vSnap-Server. Wählen Sie **Initialisieren** oder **Mit aktivierter Verschlüsselung initialisieren** aus, um Daten auf dem Server zu verschlüsseln.

Sites verwalten

Eine Site dient dazu, vSnap-Server auf der Basis einer physischen oder logischen Position zu gruppieren, um so ein schnelles Auffinden von Sicherungsdaten und die Interaktion mit Sicherungsdaten zu ermöglichen. Eine Site wird einem vSnap-Server zugeordnet, wenn der Server IBM Spectrum Protect Plus hinzugefügt wird.

Informationen zu diesem Vorgang

Eine Site wird einem vSnap-Server zugeordnet, wenn der Server IBM Spectrum Protect Plus hinzugefügt wird. Überprüfen Sie die verfügbaren Sites, indem Sie im Navigationsfenster auf **Systemkonfiguration** > **Site** klicken und festlegen, ob für Ihre vSnap-Server neue Sites hinzugefügt oder die vorhandenen editiert werden sollen.

Anmerkung: Sie können den Sitenamen und andere Optionen für die Standardsites "Primär" und "Sekundär" ändern.

Die Site "Demo" ist nur für den integrierten vSnap-Server verfügbar. Diese Site kann mit keinem anderen vSnap-Server verwendet werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Site hinzuzufügen oder zu editieren:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Site**.
2. Führen Sie die entsprechende Aktion aus, um neue Sites hinzuzufügen oder vorhandene Sites zu editieren:

Aktion	Vorgehensweise
Neue Site hinzufügen	a. Klicken Sie auf **Site hinzufügen**. b. Geben Sie einen Sitenamen ein. c. Optional: Wählen Sie **Drosselung aktivieren** aus, um den Durchsatz für Sitereplikations- und Auslagerungsoperationen zu steuern (siehe „Site hinzufügen” auf Seite 284). d. Klicken Sie auf **Speichern**.
Site editieren	a. Klicken Sie auf **Site editieren**. b. Klicken Sie auf das Symbol für Editieren  , das einer Site zugeordnet ist. c. Optional: Wählen Sie **Drosselung aktivieren** aus, um den Durchsatz für Sitereplikations- und Auslagerungsoperationen zu steuern (siehe „Site editieren” auf Seite 285). d. Klicken Sie auf **Speichern**.

Zugehörige Konzepte

„Produktkomponenten” auf Seite 1
Die IBM Spectrum Protect Plus-Lösung wird als unabhängige virtuelle Appliance bereitgestellt, die Speicher- und Datenversetzungskomponenten enthält.

„Sites verwalten” auf Seite 283
Eine *Site* ist ein IBM Spectrum Protect Plus-Richtlinienkonstrukt, das zur Steuerung der Platzierung von Daten in einer Umgebung verwendet wird.

Sicherungsrichtlinien erstellen

Sicherungsrichtlinien, die auch als SLA-Richtlinien (SLA = Service-Level-Agreement) bezeichnet werden, definieren Parameter, die auf Sicherungsjobs angewendet werden. Diese Parameter schließen die Häufigkeit und Aufbewahrung von Sicherungen ein.

Informationen zu diesem Vorgang

Die drei SLA-Standardrichtlinien sind Gold, Silber und Bronze. Sie können diese Richtlinien wie definiert verwenden oder die Richtlinien ändern. Sie können auch angepasste SLA-Richtlinien erstellen.

Wenn eine virtuelle Maschine mehreren SLA-Richtlinien zugeordnet ist, stellen Sie sicher, dass die Richtlinien nicht gleichzeitig ausgeführt werden. Planen Sie die SLA-Richtlinien so, dass zwischen der Ausführung der einzelnen Richtlinien genügend Zeit ist, oder kombinieren Sie die Richtlinien in einer einzigen SLA-Richtlinie.

Zu Beispielzwecken schließt diese Task keine Anweisungen zum Aktivieren der Replikation für vSnap-Server oder zum Auslagern oder Archivieren von Daten in sekundären Sicherungsspeicher ein, die Zusatzfunktionen sind. Informationen zum Definieren dieser Funktionen in der SLA-Richtlinie finden Sie in „SLA-Richtlinie erstellen" auf Seite 93.

Sicherungskopien von Daten werden als Momentaufnahmen bezeichnet.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine SLA-Richtlinie zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Richtlinienübersicht**.
2. Klicken Sie auf **SLA-Richtlinie hinzufügen**.

   Das Fenster **Neue SLA-Richtlinie** wird angezeigt.
3. Geben Sie in das Feld **Name** einen Namen ein, der eine aussagekräftige Beschreibung der SLA-Richtlinie bereitstellt.
4. Definieren Sie im Abschnitt **Operativer Schutz** unter **Hauptrichtlinie** die folgenden Optionen für Sicherungsoperationen. Diese Operationen werden auf den im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Platte** definierten vSnap-Servern ausgeführt.

   Aufbewahrung
   Geben Sie den Aufbewahrungszeitraum für die Sicherungsmomentaufnahmen an.

   Zeitplan inaktivieren
   Wählen Sie dieses Kontrollkästchen aus, um die Hauptrichtlinie zu erstellen, ohne eine Häufigkeit oder eine Startzeit zu definieren. Richtlinien, die ohne einen Zeitplan erstellt werden, können bedarfsgesteuert ausgeführt werden.

   Häufigkeit
   Geben Sie die Häufigkeit für Sicherungsoperationen ein.

   Startzeit
   Geben Sie das Datum und die Uhrzeit ein, an dem bzw. zu der die Sicherungsoperation gestartet werden soll.

   Zielsite
   Wählen Sie die Zielsite für die Sicherung zum Sichern von Daten aus.

   Eine Site kann einen oder mehrere vSnap-Server enthalten. Wenn eine Site mehr als einen vSnap-Server enthält, steuert der IBM Spectrum Protect Plus-Server die Datenplatzierung in den vSnap-Servern.

   In dieser Liste werden nur Sites angezeigt, die einem vSnap-Server zugeordnet sind. Sites, die IBM Spectrum Protect Plus hinzugefügt werden, aber keinem vSnap-Server zugeordnet sind, werden nicht angezeigt.

Nur verschlüsselten Plattenspeicher verwenden
Wählen Sie dieses Kontrollkästchen aus, um Daten auf verschlüsselten vSnap-Servern zu sichern, wenn Ihre Umgebung eine Kombination aus verschlüsselten und nicht verschlüsselten Servern enthält.

Einschränkung: Wenn diese Option ausgewählt wird und keine verschlüsselten vSnap-Server verfügbar sind, schlägt der zugeordnete Job fehl.

Das folgende Beispiel zeigt eine neue SLA-Richtlinie mit dem Namen `Copper`, die alle 3 Tage um Mitternacht mit einem Aufbewahrungszeitraum von 1 Monat ausgeführt wird:

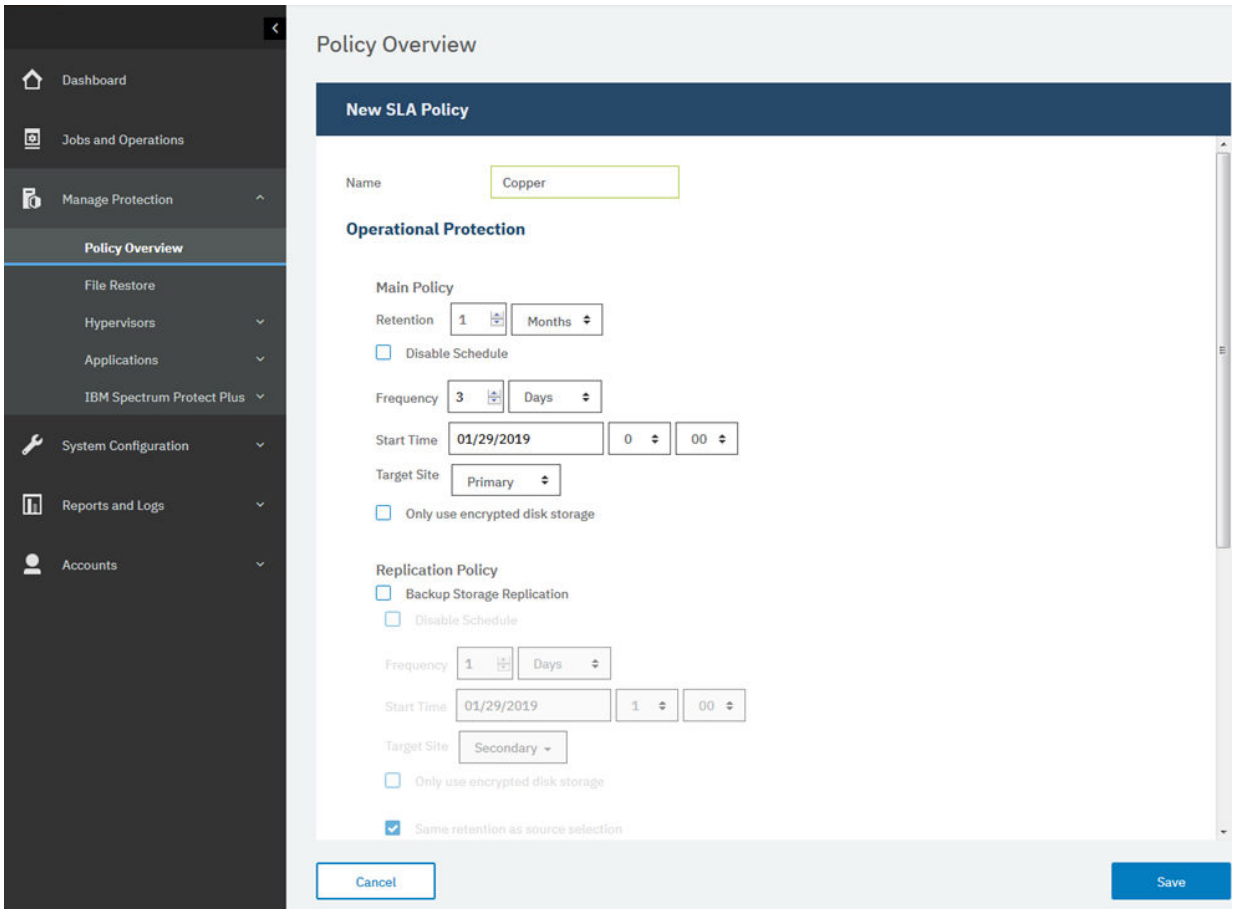


Abbildung 5. SLA-Richtlinie erstellen

5. Klicken Sie auf **Speichern**. Die SLA-Richtlinie kann jetzt wie in „Ressourcen einer Jobdefinition hinzufügen” auf Seite 81 gezeigt auf Sicherungsjobdefinitionen angewendet werden.

Zugehörige Konzepte

„Sicherungsspeicherdaten replizieren” auf Seite 5
Wenn Sie die Replikation von Sicherungsdaten aktivieren, werden Daten eines vSnap-Servers auf einem anderen vSnap-Server asynchron repliziert. Sie können beispielsweise Sicherungsdaten eines vSnap-Servers an einer primären Site auf einem vSnap-Server an einer sekundären Site replizieren.

„In sekundären Sicherungsspeicher auslagern” auf Seite 6
Der vSnap-Server ist die primäre Sicherungsposition für Momentaufnahmen. Alle IBM Spectrum Protect Plus-Umgebungen verfügen über mindestens einen vSnap-Server. Wahlweise können Sie Momentaufnahmen aus einem vSnap-Server in sekundären Sicherungsspeicher auslagern.

„SLA-Richtlinien für Sicherungsoperationen verwalten” auf Seite 93
SLA-Richtlinien (SLA = Service-Level-Agreement), die auch als Sicherungsrichtlinien bezeichnet werden, definieren Parameter für Sicherungsjobs. Diese Parameter umfassen die Häufigkeit und den Aufbewahrungszeitraum von Sicherungen sowie die Option zur Replikation oder Auslagerung von Sicherungsdaten. Sie können vordefinierte SLA-Richtlinien verwenden oder diese gemäß Ihren Anforderungen anpassen.

Benutzeraccount für den Anwendungsadministrator erstellen

Erstellen Sie einen Benutzeraccount für einen Administrator, der Sicherungs- und Zurückschreibungsoperationen für die Hypervisoren oder Anwendungen in Ihrer Umgebung ausführen kann.

Vorbereitende Schritte

Die folgenden Schritte, die als Beispiel dienen, zeigen, wie ein Account für einen einzelnen Benutzer, der für den Schutz der VMware-Daten verantwortlich ist, erstellt wird. Dieser Account verwendet eine vorhandene Benutzerrolle und Ressourcengruppe.

Informationen zum Erstellen eines Accounts für eine LDAP-Gruppe finden Sie in „Benutzeraccount für eine LDAP-Gruppe erstellen” auf Seite 320.

Informationen zum Erstellen angepasster Benutzerrollen und Ressourcengruppen finden Sie in „Ressourcengruppe erstellen” auf Seite 312 und „Rolle erstellen” auf Seite 317.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Account für einen Anwendungsadministrator zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Benutzer**.
2. Klicken Sie auf **Benutzer hinzufügen**. Das Fenster **Benutzer hinzufügen** wird angezeigt.
3. Klicken Sie auf **Typ des Benutzers oder der Gruppe auswählen, der bzw. die hinzugefügt werden soll** > **Einzelner neuer Benutzer**.
4. Geben Sie einen Namen und ein Kennwort für den Anwendungsadministrator ein.
5. Wählen Sie im Abschnitt **Rolle zuordnen** die Option **VM Admin** aus.
   Die Berechtigungen werden im Abschnitt **Berechtigungsgruppen** angezeigt.

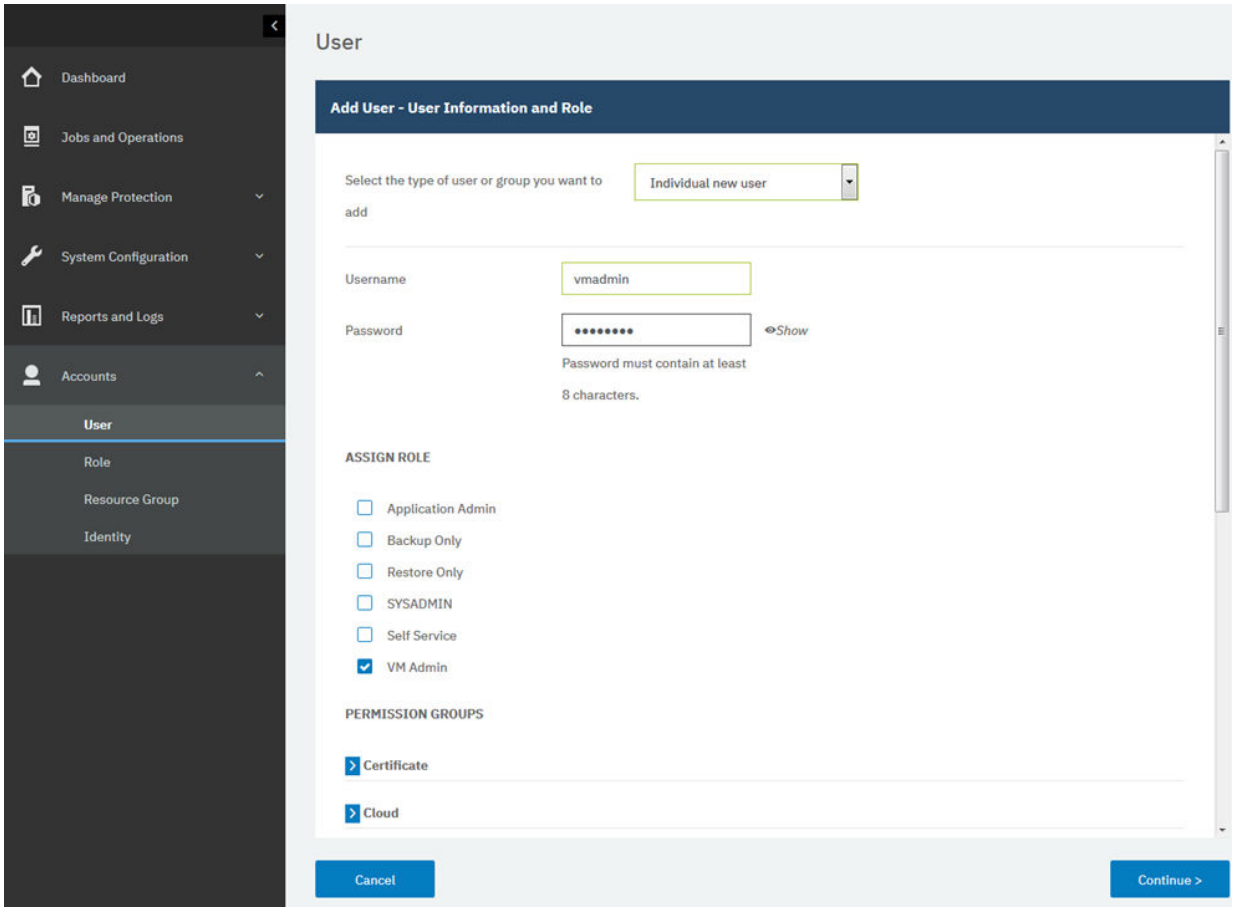


Abbildung 6. Benutzeraccount erstellen und Rolle zuordnen

6. Klicken Sie auf **Weiter**.
7. Wählen Sie im Abschnitt **Benutzer hinzufügen - Ressourcen zuordnen** die Ressourcengruppe **Alle Ressourcen** aus und klicken Sie dann auf **Ressourcen hinzufügen**.

   Die Ressourcengruppe wird dem Abschnitt **Ausgewählte Ressourcen** hinzugefügt.

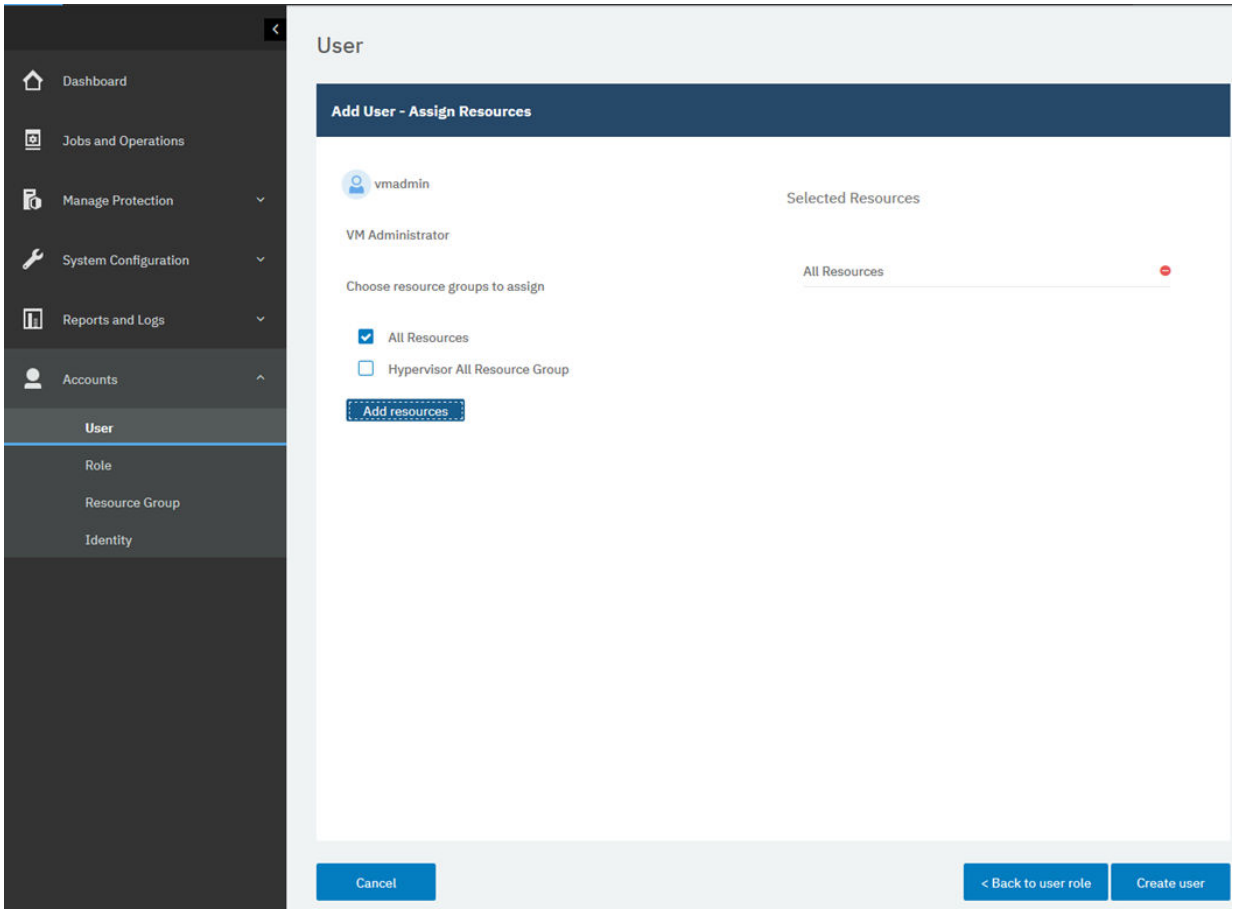


Abbildung 7. Ressourcengruppe für den Benutzeraccount auswählen

8. Klicken Sie auf **Benutzer erstellen**.

Zugehörige Konzepte

„Benutzerzugriff verwalten" auf Seite 311
Sie können mithilfe der rollenbasierten Zugriffssteuerung die Ressourcen und Berechtigungen festlegen, die IBM Spectrum Protect Plus-Benutzeraccounts zur Verfügung stehen.

Zu schützende Ressourcen hinzufügen

Ressourcen sind Server für Hypervisoren oder Anwendungen, auf denen Daten gehostet werden, die geschützt werden sollen. Nachdem eine Ressource registriert wurde, wird ein Bestand der Ressource erfasst und dem IBM Spectrum Protect Plus-Bestand hinzugefügt. Damit wird es Ihnen ermöglicht, Sicherungs- und Zurückschreibungsjobs auszuführen und Berichte zu erstellen.

Informationen zu diesem Vorgang

Als Beispiel wird in dieser Task beschrieben, wie eine VMware-Ressource hinzugefügt wird. Um andere Ressourcen hinzuzufügen, lesen Sie die Anweisungen nach Ressourcentyp in Kapitel 7, „Hypervisoren schützen", auf Seite 99 und Kapitel 8, „Anwendungen schützen", auf Seite 143.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine vCenter Server-Instanz hinzuzufügen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **VMware**.
2. Klicken Sie auf **vCenter verwalten** und dann auf **vCenter hinzufügen**.
3. Füllen Sie die Felder im Abschnitt **vCenter-Eigenschaften** aus:

Hostname/IP
Geben Sie die auflösbare IP-Adresse oder einen auflösbaren Pfad und Maschinennamen ein.

Vorhandenen Benutzer verwenden
Aktivieren Sie dieses Feld, um einen zuvor eingegebenen Benutzernamen und ein zuvor eingegebenes Kennwort für die vCenter Server-Instanz auszuwählen.

Benutzername
Geben Sie Ihren Benutzernamen für die vCenter Server-Instanz ein.

Kennwort
Geben Sie Ihr Kennwort für die vCenter Server-Instanz ein.

Port
Geben Sie den Kommunikationsport der vCenter Server-Instanz ein. Wählen Sie das Kontrollkästchen **SSL verwenden** aus, um eine verschlüsselte Secure Sockets Layer-Verbindung (SSL-Verbindung) zu aktivieren. Der Standardport ist 80 für Nicht-SSL-Verbindungen und 443 für SSL-Verbindungen.

4. Konfigurieren Sie im Abschnitt **Optionen** die folgende Option:

Maximale Anzahl VMs, die pro ESX-Server und pro SLA gleichzeitig verarbeitet werden sollen
Definieren Sie die maximale Anzahl der VM-Momentaufnahmen, die auf dem ESX-Server gleichzeitig verarbeitet werden sollen.

Das folgende Beispiel zeigt die ausgefüllten Felder.

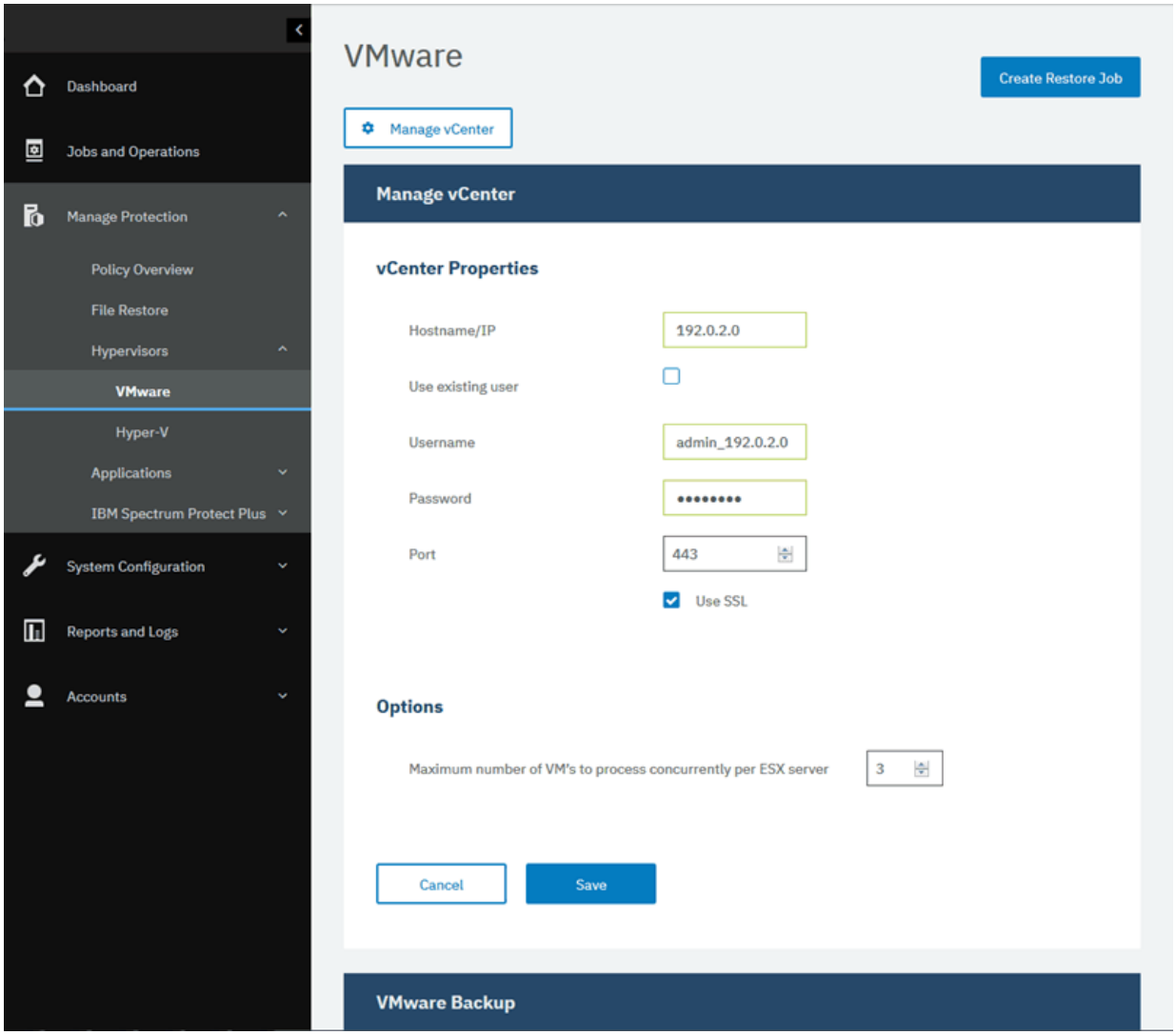


Abbildung 8. vCenter Server-Instanz hinzufügen

5. Klicken Sie auf **Speichern**.

   IBM Spectrum Protect Plus bestätigt eine Netzverbindung, fügt die Ressource zur Datenbank hinzu und katalogisiert dann die Ressource. Wird eine Nachricht angezeigt, die angibt, dass die Verbindung nicht erfolgreich ist, überprüfen Sie Ihre Eingaben. Sind Ihre Eingaben korrekt und ist die Verbindung nicht erfolgreich, bitten Sie einen Netzadministrator, die Verbindungen zu überprüfen und nach Möglichkeit zu korrigieren.

Ressourcen einer Jobdefinition hinzufügen

Bevor Sie eine Ressource sichern können, müssen Sie eine Jobdefinition erstellen, die die Ressource einer oder mehreren Sicherungsrichtlinien, die auch als SLA-Richtlinien bezeichnet werden, zuordnet.

Informationen zu diesem Vorgang

Als Beispiel wird in dieser Task beschrieben, wie eine SLA-Richtlinie für Ressourcen ausgewählt wird, die sich in einem VMware vCenter befinden. Um eine Richtlinie für andere Ressourcen auszuwählen, lesen Sie die Anweisungen nach Ressourcentyp in Kapitel 7, „Hypervisoren schützen", auf Seite 99 und Kapitel 8, „Anwendungen schützen", auf Seite 143.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine SLA-Richtlinie auszuwählen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **VMware**.
2. Wählen Sie die Ressourcen aus, die gesichert werden sollen. Sie können alle Ressourcen in einem vCenter auswählen oder ein Drilldown durchführen, um bestimmte Ressourcen auszuwählen.

   Verwenden Sie die Suchfunktion, um nach verfügbaren Ressourcen zu suchen, und wechseln Sie mithilfe des Filters **Sicht** zwischen den angezeigten Ressourcen. Verfügbare Optionen sind **VMs und Schablonen**, **VMs**, **Datenspeicher**, **Tags und Kategorien** und **Hosts und Cluster**. Tags, die in vSphere angewendet werden, ermöglichen das Zuordnen von Metadaten zu virtuellen Maschinen.

   Das folgende Beispiel zeigt eine spezifische Festplatte, die für die Sicherung ausgewählt wurde:

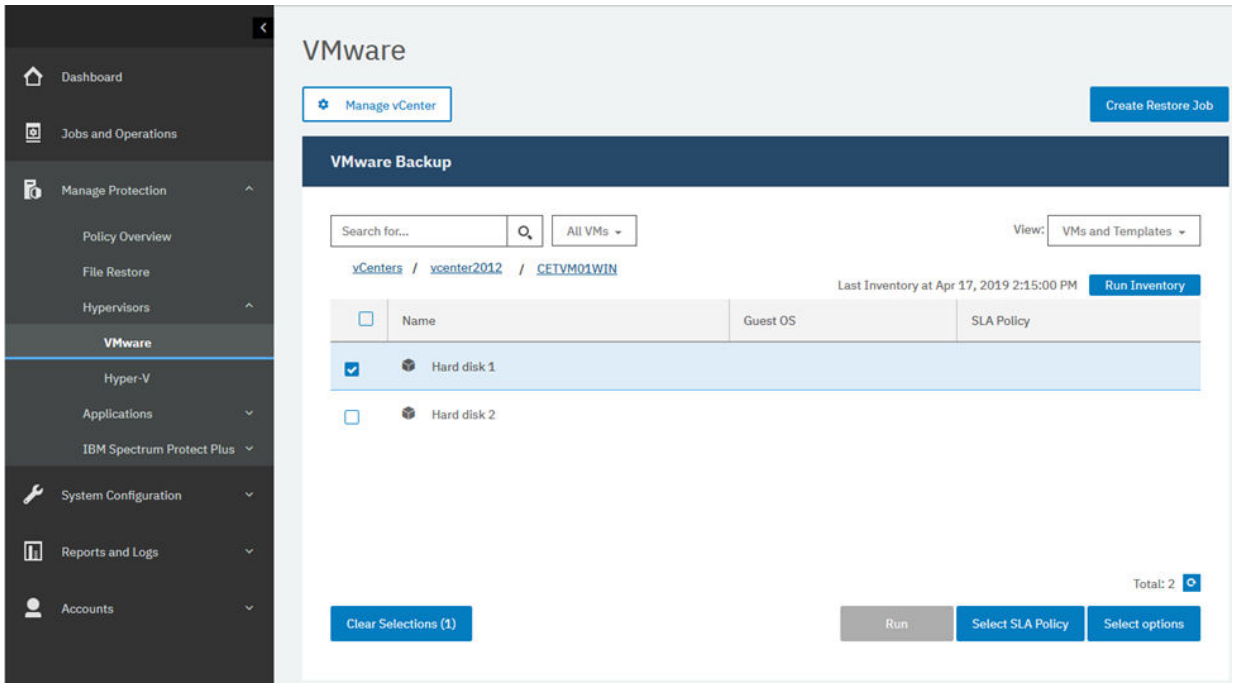


Abbildung 9. Ressourcen für die Sicherung auswählen

3. Klicken Sie auf **SLA-Richtlinie auswählen**, um eine oder mehrere SLA-Richtlinien, die Ihre Sicherungsdatenkriterien erfüllen, zur Jobdefinition hinzuzufügen.

   Das folgende Beispiel zeigt die ausgewählte SLA-Richtlinie **Copper**:

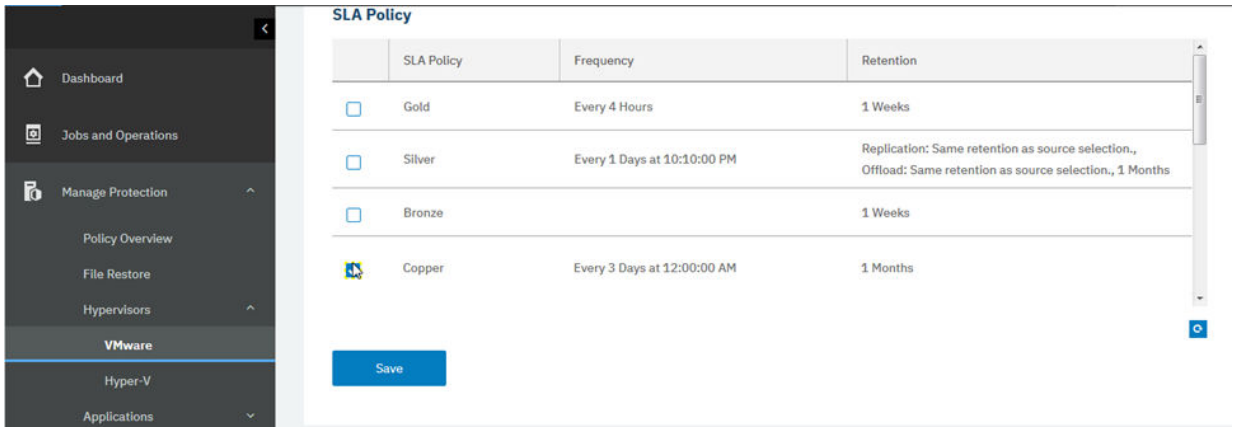


Abbildung 10. SLA-Richtlinie auswählen

4. Um die Jobdefinition mithilfe von Standardoptionen zu erstellen, klicken Sie auf **Speichern**.
5. Optional: Um zusätzliche Optionen zu konfigurieren, klicken Sie auf **Optionen auswählen** und führen Sie die Anweisungen in „VMware-Daten sichern” auf Seite 107 aus.
6. Klicken Sie auf **Speichern**.

Nachdem die Jobdefinition gespeichert wurde, werden verfügbare Platten virtueller Maschinen (VMDKs) in einer virtuellen Maschine erkannt und angezeigt, wenn **VMs und Schablonen** im Filter **Sicht** ausgewählt wird. Standardmäßig werden diese VMDKs derselben SLA-Richtlinie wie die virtuelle Maschine zugeordnet. Um eine differenziertere Richtlinie durch den Ausschluss einzelner VMDKs zu definieren, führen Sie wahlweise die Anweisungen in „VMDKs aus der SLA-Richtlinie für einen Job ausschließen” auf Seite 111 aus.

Ergebnisse

Der Job wird wie mit den von Ihnen ausgewählten SLA-Richtlinien definiert ausgeführt; Sie können den Job auch manuell ausführen, indem Sie auf **Jobs und Operationen** und dann auf die Registerkarte **Richtlinien- und Jobliste** klicken. Anweisungen finden Sie in „Sicherungsjob starten” auf Seite 83.

Zugehörige Konzepte

„IBM Spectrum Protect Plus schützen” auf Seite 259

Zum Schutz der IBM Spectrum Protect Plus-Anwendung sichern Sie die zugrunde liegenden Datenbanken für Wiederherstellungsszenarios. Konfigurationseinstellungen, registrierte Ressourcen, Zurückschreibungspunkte, Sicherungsspeichereinstellungen, Suchdaten sowie Jobinformationen werden auf einem vSnap-Server gesichert, der in der zugeordneten SLA-Richtlinie definiert ist.

Sicherungsjob starten

Sie können einen Sicherungsjob bedarfsgesteuert außerhalb des Zeitplans starten, der durch die SLA-Richtlinie definiert ist.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen bedarfsgesteuerten Sicherungsjob zu starten:

1. Klicken Sie im Navigationsfenster auf **Jobs und Operationen** und öffnen Sie die Registerkarte **Zeitplan**.

   Wenn Ihr Job kein geplanter Job, sondern ein bedarfsgesteuerter Job ist, klicken Sie auf die Registerkarte **Jobprotokoll**.
2. Wählen Sie den Job aus, der ausgeführt werden soll, und klicken Sie auf **Aktionen** > **Starten**.

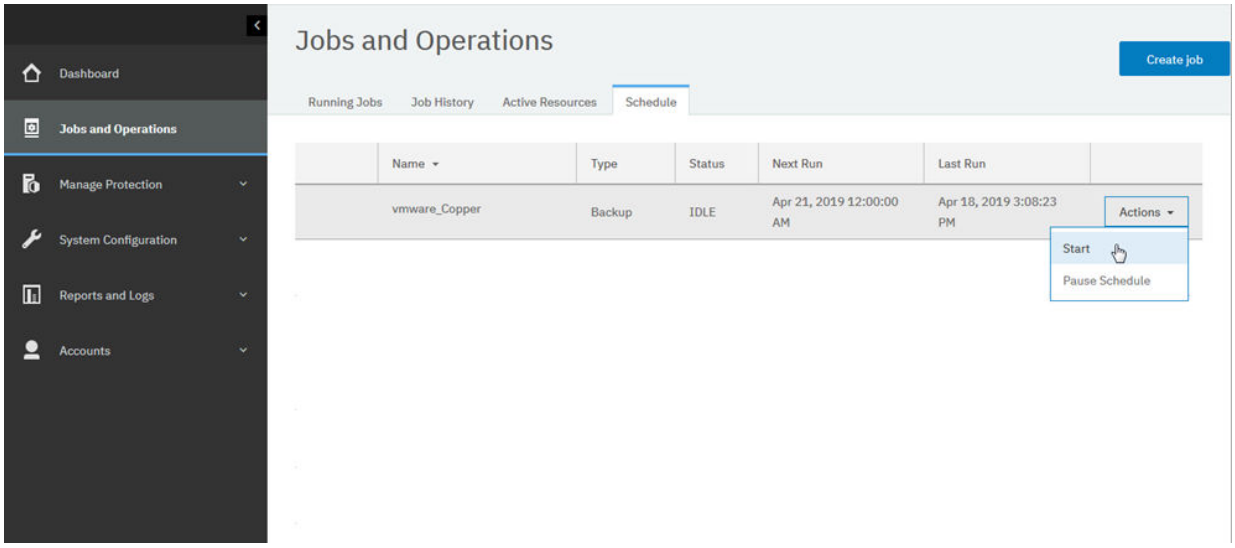


Abbildung 11. Job starten

3. Um das Jobprotokoll detailliert anzuzeigen, klicken Sie auf der Registerkarte **Aktive Jobs** auf den Job.

   In der Protokollanzeige werden die folgenden Details angezeigt:

- Status: Zeigt an, ob es sich bei der Nachricht um eine Fehler-, Warn- oder Informationsnachricht handelt.
- Zeit: Zeigt die Zeitmarke der Nachricht an.
- ID: Zeigt die eindeutige ID für die Nachricht an, sofern zutreffend.
- Beschreibung: Zeigt den Text der Nachricht an.

4. Sie können ein Jobprotokoll von der Seite herunterladen, indem Sie auf **ZIP-Datei herunterladen** klicken. Wenn der Job abgebrochen werden soll, klicken Sie auf **Aktionen** > **Abbrechen**.
5. Klicken Sie auf das Menü **Aktionen**, das dem Job zugeordnet ist, der gestartet werden soll, und klicken Sie auf **Starten** (siehe das folgende Beispiel):

Zugehörige Konzepte

„Jobs und Operationen” auf Seite 263
Verwenden Sie das Fenster **Jobs und Operationen**, um Jobs zu überwachen, das Jobprotokoll zu überprüfen, Jobs zu planen, aktive Ressourcen anzuzeigen und Jobs und Zeitpläne erneut auszuführen oder anzuhalten.

Bericht ausführen

Führen Sie Berichte mit vordefinierten Standardparametern oder mit angepassten Parametern aus.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Bericht auszuführen:

1. Klicken Sie im Navigationsfenster auf **Berichte und Protokolle** > **Berichte**.
2. Erweitern Sie einen Berichtstyp und wählen Sie einen Bericht aus, der ausgeführt werden soll (siehe das folgende Beispiel):

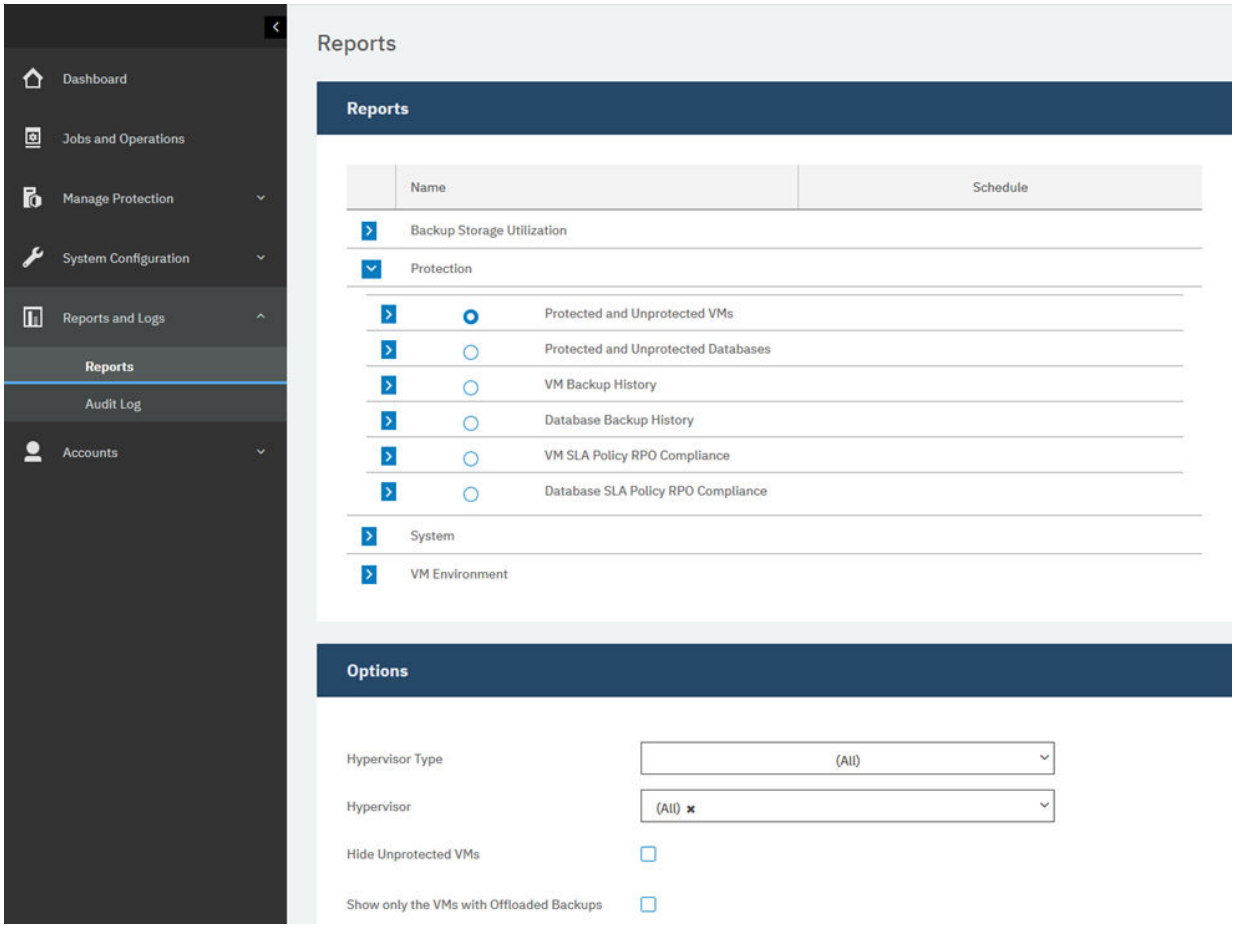


Abbildung 12. Auszuführenden Bericht auswählen

3. Führen Sie den Bericht entweder mit angepassten Parametern oder mit Standardparametern aus:
   - Um den Bericht mit angepassten Parametern auszuführen, legen Sie die Parameter im Abschnitt **Optionen** fest und klicken Sie auf **Ausführen**. Parameter sind für jeden Bericht eindeutig.
   - Um den Bericht mit Standardparametern auszuführen, klicken Sie auf **Ausführen**.

Zugehörige Konzepte

„Berichte und Protokolle verwalten” auf Seite 303

IBM Spectrum Protect Plus stellt eine Reihe vordefinierter Berichte bereit, die Sie Ihren Berichtsanforderungen entsprechend anpassen können. Darüber hinaus wird ein Protokoll der Aktionen bereitgestellt, die Benutzer in IBM Spectrum Protect Plus ausführen.

Kapitel 5. IBM Spectrum Protect Plus-Komponenten aktualisieren

Sie können die virtuelle IBM Spectrum Protect Plus-Appliance, vSnap-Server und die VADP-Proxy-Server aktualisieren, um die neuesten Funktionen und funktionalen Erweiterungen zu erhalten. Software-Patches und -Updates werden mithilfe der Verwaltungskonsole von IBM Spectrum Protect Plus oder mithilfe der Befehlszeilenschnittstelle für diese Komponenten installiert.

Informationen zu verfügbaren Aktualisierungsdateien und wie diese von einer IBM Downloads-Site abgerufen werden finden Sie in Technote 879861.

Vor einer Aktualisierung der IBM Spectrum Protect Plus-Komponenten müssen Sie die Hardware- und Softwareanforderungen für die Komponenten überprüfen, um festzustellen, ob es seit der vorherigen Version Änderungen gegeben hat.

Beachten Sie die folgenden Einschränkungen und Tipps:

- Sie müssen vSnap-Server, die sich nicht in virtuellen Appliances von IBM Spectrum Protect Plus befinden, separat aktualisieren.
- Bei einem Aktualisierungsprozess über die Verwaltungskonsole werden IBM Spectrum Protect Plus-Funktionen und die zugrunde liegenden Infrastrukturkomponenten, einschließlich Betriebssystem und Dateisystem, aktualisiert. Verwenden Sie keine andere Methode zur Aktualisierung dieser Komponenten.
- Führen Sie eine Aktualisierung der zugrunde liegenden Komponenten für IBM Spectrum Protect Plus nur dann durch, wenn die Komponente in einem IBM Spectrum Protect Plus-Aktualisierungspaket bereitgestellt wird. Infrastrukturaktualisierungen werden von IBM Aktualisierungsfunktionen gesteuert. Die Verwaltungskonsole ist die primäre Methode zur Aktualisierung der IBM Spectrum Protect Plus-Funktionen und der zugrunde liegenden Infrastrukturkomponenten, einschließlich Betriebssystem und Dateisystem.

Führen Sie die folgenden Aktionen aus:

- Vor der Aktualisierung von Komponenten müssen Sie Ihre IBM Spectrum Protect Plus-Umgebung wie in „IBM Spectrum Protect Plus-Anwendung sichern” auf Seite 259 beschrieben sichern.
- Nach einer Aktualisierung von IBM Spectrum Protect Plus kann ohne eine VM-Momentaufnahme kein Rollback auf eine vorherige Version durchgeführt werden. Erstellen Sie eine VM-Momentaufnahme von Ihrer Umgebung, bevor Sie IBM Spectrum Protect Plus aktualisieren. Wenn später ein Rollback von IBM Spectrum Protect Plus auf eine vorherige Version durchgeführt werden soll, benötigen Sie eine VM-Momentaufnahme. Wenn das Upgrade erfolgreich ausgeführt wurde, können Sie die VM-Momentaufnahme entfernen.

Virtuelle IBM Spectrum Protect Plus-Appliance aktualisieren

Aktualisieren Sie die virtuelle Appliance mithilfe der IBM Spectrum Protect Plus-Verwaltungskonsole. Die Aktualisierung von IBM Spectrum Protect Plus kann offline oder - wenn Sie über externen Internetzugriff verfügen - online ausgeführt werden.

Vorbereitende Schritte

Sie können IBM Spectrum Protect Plus Version 10.1.2 oder höher direkt auf die aktuelle Version aktualisieren. Wenn Sie Version 10.1.1 verwenden, müssen Sie eine Aktualisierung auf Version 10.1.2 und dann eine Aktualisierung auf die aktuelle Version durchführen. Anweisungen zur Durchführung einer Aktualisierung von Version 10.1.1 auf Version 10.1.2 finden Sie in Updating the IBM Spectrum Protect Plus virtual appliance to version 10.1.2.

Führen Sie vor dem Start des Aktualisierungsprozesses die folgenden Schritte aus:

© Copyright IBM Corp. 2017, 2019

1. Stellen Sie sicher, dass Ihre IBM Spectrum Protect Plus-Umgebung gesichert wurde, bevor Sie Aktualisierungen ausführen. Weitere Informationen zum Sichern Ihrer Umgebung finden Sie in „IBM Spectrum Protect Plus-Anwendung sichern” auf Seite 259.
2. Laden Sie für Offlineaktualisierungen die vorausgesetzte IBM Spectrum Protect Plus-Aktualisierung mit dem Namen `CC1QHML.iso` in ein Verzeichnis auf dem Computer herunter, auf dem der Browser für die Verwaltungskonsole ausgeführt wird. Die Aktualisierungsdatei wird zuerst installiert.
3. Stellen Sie sicher, dass keine Jobs während der Aktualisierungsprozedur ausgeführt werden. Halten Sie den Zeitplan für alle Jobs an, deren Status INAKTIV oder ABGESCHLOSSEN lautet.

Eine Liste der Download-Images, einschließlich des erforderlichen Betriebssystemupdates für die virtuelle Appliance, finden Sie in Technote 879861.

Informationen zu diesem Vorgang

Wenn Sie über Internetzugriff verfügen, können Sie die Aktualisierungsprozedur wahlweise online ausführen. Wenn Sie nicht über Internetzugriff verfügen, können Sie die Aktualisierungsprozedur offline ausführen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die virtuelle IBM Spectrum Protect Plus-Appliance zu aktualisieren:

1. Greifen Sie über einen unterstützten Web-Browser auf die Verwaltungskonsole zu, indem Sie die folgenden Adresse eingeben:

   ```
   https://Hostname:8090/
   ```

   Dabei ist *Hostname* die IP-Adresse der virtuellen Maschine, auf der die Anwendung implementiert ist.
2. Wählen Sie im Anmeldefenster einen der folgenden Authentifizierungstypen in der Liste **Authentifizierungstyp** aus:

Authentifizierungstyp	Anmeldeinformationen
IBM Spectrum Protect Plus	Um sich als IBM Spectrum Protect Plus-Benutzer mit SYSADMIN-Berechtigungen anzumelden, geben Sie Ihren Administratorbenutzernamen und Ihr Kennwort ein. Wenn Sie sich unter Verwendung des Benutzeraccounts `admin` anmelden, werden Sie zum Zurücksetzen des Benutzernamens und des Kennworts aufgefordert. Sie können den Benutzernamen nicht auf `admin`, `root` oder `test` zurücksetzen.
System (empfohlen)	Um sich als Systembenutzer anzumelden, geben Sie die Benutzer-ID "serveradmin" ein. Das Standardkennwort ist `sppDP758`. Sie werden bei der ersten Anmeldung aufgefordert, dieses Kennwort zu ändern.

3. Klicken Sie auf **Management von Aktualisierungen und Hotfixes**, um die Seite für das Management von Aktualisierungen zu öffnen.

   Wenn Sie über Zugriff auf die FTP-Site public.dhe.ibm.com, verfügen, prüft die Administratorkonsole automatisch auf verfügbare Aktualisierungen und listet diese auf.
4. Klicken Sie auf **Aktualisierung ausführen**, um die verfügbaren Aktualisierungen zu installieren.
   - Nachdem die Aktualisierungen erfolgreich installiert wurden, fahren Sie mit Schritt 6 fort.
   - Wenn Sie planen, eine Aktualisierung von einer ISO-Datei zu installieren, klicken Sie auf **Auf diese Stelle klicken**, um die Offlineaktualisierungen auszuführen. Fahren Sie mit Schritt 5 fort.

Anmerkung: Wenn Onlineaktualisierungen ausgeführt werden sollen, aber nur der Offlinemodus angezeigt wird, überprüfen Sie Ihre Internetkonnektivität und versuchen Sie erneut, auf die FTP-Site public.dhe.ibm.com zuzugreifen.

5. Wählen Sie die Aktualisierung, die ausgeführt werden soll, wie folgt aus:
   - Onlinemodus: Aktualisierungen werden automatisch im Repository aufgelistet, sobald sie verfügbar gemacht werden. Klicken Sie auf **Aktualisierung ausführen**.
   - Offlinemodus: Klicken Sie auf **Datei auswählen**, um nach der heruntergeladenen Datei zu suchen. Die Datei hat eine Erweiterung `iso` oder `rpm` wie in dem folgenden Beispiel: `<Dateiname>.iso`. Klicken Sie auf **Update-Image (oder) Hotfix hochladen**.

     Anmerkung: Sie können jeweils nur eine einzige Aktualisierungsdatei auswählen.

   Wenn die Aktualisierung abgeschlossen ist, wird die virtuelle Maschine, auf der die Anwendung implementiert ist, automatisch erneut gestartet.

   Wichtig: Nachdem die IBM Spectrum Protect Plus-Aktualisierung abgeschlossen ist, müssen Sie alle externen vSnap- und VADP-Proxy-Server in Ihrer Umgebung aktualisieren.
6. Löschen Sie den Browser-Cache.

   Unter Umständen ist HTML-Inhalt von Vorgängerversionen von IBM Spectrum Protect Plus in dem Cache gespeichert.
7. Starten Sie die aktualisierte Version von IBM Spectrum Protect Plus.
8. Klicken Sie im Navigationsfenster auf **Jobs und Operationen** und klicken Sie dann auf die Registerkarte **Zeitplan**.

   Suchen Sie nach den Jobs, die angehalten wurden.
9. Wählen Sie im Menü **Aktionen** für die angehaltenen Jobs **Zeitplan freigeben** aus.

Zugehörige Tasks

„vSnap-Server aktualisieren” auf Seite 89
Der Standard-vSnap-Server wird mit der IBM Spectrum Protect Plus-Appliance aktualisiert. Sie müssen alle zusätzlichen vSnap-Server, die auf virtuellen oder physischen Appliances installiert sind, separat aktualisieren.

vSnap-Server aktualisieren

Der Standard-vSnap-Server wird mit der IBM Spectrum Protect Plus-Appliance aktualisiert. Sie müssen alle zusätzlichen vSnap-Server, die auf virtuellen oder physischen Appliances installiert sind, separat aktualisieren.

Vorbereitende Schritte

Sie können für Ihre vSnap-Server direkt eine Aktualisierung von Version 10.1.2 oder höher auf die aktuelle Version durchführen. Wenn Sie Version 10.1.1 verwenden, müssen Sie eine Aktualisierung auf Version 10.1.2 und dann eine Aktualisierung auf die aktuelle Version durchführen. Anweisungen zur Durchführung einer Aktualisierung auf Version 10.1.2, finden Sie in Updating vSnap servers to version 10.1.2.

Testzurückschreibungsjobs müssen abgeschlossen sein, bevor eine Aktualisierung für vSnap gestartet wird. Jobs, die nicht abgeschlossen sind oder abgebrochen werden, wenn eine Aktualisierung gestartet wird, sind nicht sichtbar, sobald die Aktualisierung abgeschlossen ist. Wenn Jobs nach dem Abschluss der Aktualisierung nicht sichtbar sind, führen Sie erneut Testzurückschreibungsjobs aus.

Unter Umständen ist es auch erforderlich, das Betriebssystem für die vSnap-Server zu aktualisieren, bevor die Server aktualisiert werden. Informationen zu Betriebssystemanforderungen finden Sie in „Komponentenanforderungen” auf Seite 11.

Führen Sie die folgenden Schritte aus, um die aktuelle Version und das Betriebssystem für Ihre vSnap-Server zu überprüfen:

1. Melden Sie sich beim vSnap-Server als Benutzer `serveradmin` an. Wenn Sie IBM Spectrum Protect Plus 10.1.1 verwenden, melden Sie sich unter Verwendung des Root-Accounts an.
2. Um die Version des vSnap-Servers und das Betriebssystem zu überprüfen, geben Sie über die vSnap-Befehlszeilenschnittstelle den folgenden Befehl aus:

```
vsnap system info
```

Stellen Sie sicher, dass keine Jobs, die den vSnap-Server verwenden, während der Aktualisierungsprozedur aktiv sind. Halten Sie den Zeitplan für alle Jobs an, deren Status INAKTIV oder ABGESCHLOSSEN lautet.

Betriebssystem für einen physischen vSnap-Server aktualisieren

Wenn der vSnap-Server auf einer Maschine installiert ist, die Red Hat Enterprise Linux ausführt, müssen Sie das Betriebssystem auf Version 7.5 oder 7.6 aktualisieren, bevor Sie den vSnap-Server aktualisieren. Anweisungen zur Aktualisierung des Betriebssystems finden Sie in der Red Hat Enterprise Linux-Dokumentation.

Zugehörige Tasks

„vSnap-Server aktualisieren” auf Seite 90

Der Standard-vSnap-Server wird mit der IBM Spectrum Protect Plus-Appliance aktualisiert. Sie müssen alle zusätzlichen vSnap-Server, die auf virtuellen oder physischen Appliances installiert sind, separat aktualisieren.

Betriebssystem für einen virtuellen vSnap-Server aktualisieren

Wenn es sich bei dem Betriebssystem um CentOS Linux Version 7.4 oder früher handelt, müssen Sie das Betriebssystem aktualisieren, bevor Sie den vSnap-Server aktualisieren. Um das Betriebssystem zu aktualisieren, führen Sie die Anweisungen in Updating vSnap servers to version 10.1.2 aus. Die Installation der Version 10.1.2 umfasst CentOS Linux Version 7.5.

Zugehörige Tasks

„vSnap-Server aktualisieren” auf Seite 90

Der Standard-vSnap-Server wird mit der IBM Spectrum Protect Plus-Appliance aktualisiert. Sie müssen alle zusätzlichen vSnap-Server, die auf virtuellen oder physischen Appliances installiert sind, separat aktualisieren.

vSnap-Server aktualisieren

Der Standard-vSnap-Server wird mit der IBM Spectrum Protect Plus-Appliance aktualisiert. Sie müssen alle zusätzlichen vSnap-Server, die auf virtuellen oder physischen Appliances installiert sind, separat aktualisieren.

Vorbereitende Schritte

Führen Sie vor dem Start des Aktualisierungsprozesses die folgenden Schritte aus:

1. Stellen Sie sicher, dass Sie Ihre IBM Spectrum Protect Plus-Umgebung wie in „IBM Spectrum Protect Plus-Anwendung sichern” auf Seite 259 beschrieben gesichert haben.
2. Wenn Sie eine Aktualisierung von IBM Spectrum Protect Plus 10.1.1 durchführen, müssen Sie eine Aktualisierung auf Version 10.1.2 und dann eine Aktualisierung auf die aktuelle Version durchführen. Anweisungen zur Durchführung einer Aktualisierung auf Version 10.1.2, finden Sie in Updating vSnap servers to version 10.1.2.
3. Laden Sie die vSnap-Aktualisierungsdatei `CC1QGML.run` herunter und kopieren Sie sie in ein temporäres Verzeichnis auf dem vSnap-Server. Informationen zum Herunterladen von Dateien finden Sie in Technote 879861.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen vSnap-Server zu aktualisieren:

1. Melden Sie sich beim vSnap-Server als Benutzer **serveradmin** an.

2. Ändern Sie in dem Verzeichnis, in dem sich die Datei `CC1QGML.run` befindet, die Datei in eine ausführbare Datei und führen Sie das Installationsprogramm aus, indem Sie die folgenden Befehle ausgeben:

```
chmod +x CC1QGML.run
```

```
sudo ./CC1QGML.run
```

   Die vSnap-Pakete werden installiert.
3. Starten Sie die aktualisierte Version von IBM Spectrum Protect Plus.
4. Klicken Sie im Navigationsfenster auf **Jobs und Operationen** und klicken Sie dann auf die Registerkarte **Zeitplan**.

   Suchen Sie nach den Jobs, die angehalten wurden.
5. Wählen Sie im Menü **Aktionen** für die angehaltenen Jobs **Zeitplan freigeben** aus.

VADP-Proxys aktualisieren

Durch die Aktualisierung der virtuellen IBM Spectrum Protect Plus-Appliance werden automatisch alle VADP-Proxys aktualisiert, die der virtuellen Appliance zugeordnet sind. In seltenen Szenarios, wie beispielsweise dem Verlust der Netzkonnektivität, müssen Sie den VADP-Proxy manuell aktualisieren.

Vorbereitende Schritte

Stellen Sie zunächst sicher, dass Sie Ihre IBM Spectrum Protect Plus-Umgebung wie in „IBM Spectrum Protect Plus-Anwendung sichern” auf Seite 259 beschrieben gesichert haben.

Vorgehensweise

Wenn eine VADP-Proxy-Aktualisierung für externe Proxys während eines Neustarts der virtuellen IBM Spectrum Protect Plus-Appliance verfügbar ist, wird die Aktualisierung automatisch auf jeden VADP-Proxy angewendet, der einer Identität zugeordnet ist. Um einen VADP-Proxy einer Identität zuzuordnen, navigieren Sie zu **Systemkonfiguration** > **VADP-Proxy**. Klicken Sie auf das Symbol für Optionen ••• und wählen Sie **Optionen definieren** aus. Wählen Sie über die Einstellung "Benutzer" einen zuvor eingegebenen Benutzernamen und das zugehörige Kennwort für den VADP-Proxy-Server aus.

Führen Sie die folgenden Schritte aus, um einen VADP-Proxy manuell zu aktualisieren:

1. Navigieren Sie zur Seite **Systemkonfiguration** > **VADP-Proxy** in IBM Spectrum Protect Plus.
2. Auf der Seite **VADP-Proxy** wird jeder Proxy-Server angezeigt. Wenn eine neuere Version der VADP-Proxy-Software verfügbar ist, wird ein Symbol für Aktualisieren im Feld **Status** angezeigt.
3. Stellen Sie sicher, dass keine aktiven Jobs vorhanden sind, die den Proxy verwenden, und klicken Sie dann auf das Symbol für Aktualisieren.

   Der Proxy-Server wechselt in den Aussetzstatus und installiert die neueste Aktualisierung. Wenn die Aktualisierung abgeschlossen ist, wird der VADP-Proxy-Server automatisch wiederaufgenommen und wechselt in den Status "Aktiviert".

Wenn Sie versuchen, als Benutzer ohne Rootberechtigung eine Aktualisierung durchzuführen, müssen bestimmte Anweisungen beachtet werden, wenn eine Push-Installation oder Push-Aktualisierung für einen VADP-Proxy ausgeführt werden soll.

1. Erstellen Sie eine Datei im Verzeichnis /etc/sudoers.d/.

```
sudo cd /etc/sudoers.d/
```

2. Schreiben Sie den Text in die Datei und speichern Sie diese, indem Sie nach der Eingabe des Textes strg+d auf der Tastatur drücken.

```
sudo cat > 99-vadpuser
     Defaults !requiretty
```

```
     vadpuser ALL=NOPASSWD: /tmp/cdm_guestapps_vadpuser/runcommand.sh
<<strg+d>> drücken
```

3. Definieren Sie die entsprechenden Berechtigungen für die Datei.

```
sudo chmod 0440 99-vadpuser
```

Nächste Schritte

Führen Sie nach dem Aktualisieren der VADP-Proxys die folgende Aktion aus:

Aktion	Vorgehensweise
Führen Sie den VMware-Sicherungsjob aus.	Siehe „VMware-Daten sichern” auf Seite 107. Die Proxys werden im Jobprotokoll durch eine ähnliche Protokollnachricht wie die folgende angegeben: `Run remote vmdkbackup of MicroService: http://<Proxy` *`Knotenname`*`, IP:`*`IP-Adresse_des_Proxys`*

Zugehörige Tasks

„VADP-Proxys erstellen” auf Seite 113
Sie können VADP-Proxys für die Ausführung von VMware-Sicherungsjobs mit IBM Spectrum Protect Plus in Linux-Umgebungen erstellen.

Zugehörige Verweise

„Firewall-Ports editieren” auf Seite 51
Verwenden Sie die bereitgestellten Beispiele als Referenz, um Firewall-Ports auf fernen VADP-Proxy-Servern oder Anwendungsservern zu öffnen. Sie müssen den Portdatenverkehr auf das erforderliche Netz oder die erforderlichen Adapter beschränken.

Vorabverfügbarkeitsaktualisierungen anwenden

Vorabverfügbarkeitsaktualisierungen stellen Fixes für APARs (Authorized Program Analysis Reports) und kleinere Probleme zwischen IBM Spectrum Protect Plus-Releases zur Verfügung. Diese Aktualisierungen sind in Paketen über die Website von Fix Central Online verfügbar.

Informationen zu diesem Vorgang

Vorabverfügbarkeitsaktualisierungen enthalten möglicherweise nicht Fixes für alle IBM Spectrum Protect Plus-Komponenten.

Anweisungen zum Abrufen und Installieren vorläufiger Fixes finden Sie in den Downloadinformationen, die veröffentlicht werden, sobald die Fixes verfügbar sind.

Kapitel 6. SLA-Richtlinien für Sicherungsoperationen verwalten

SLA-Richtlinien (SLA = Service-Level-Agreement), die auch als Sicherungsrichtlinien bezeichnet werden, definieren Parameter für Sicherungsjobs. Diese Parameter umfassen die Häufigkeit und den Aufbewahrungszeitraum von Sicherungen sowie die Option zur Replikation oder Auslagerung von Sicherungsdaten. Sie können vordefinierte SLA-Richtlinien verwenden oder diese gemäß Ihren Anforderungen anpassen.

Die folgenden SLA-Standardrichtlinien sind verfügbar. Jede Richtlinie gibt eine Häufigkeit und einen Aufbewahrungszeitraum für die Sicherung an. Sie können diese Richtlinien unverändert übernehmen oder ändern. Sie können auch angepasste SLA-Richtlinien erstellen.

Gold
Diese Richtlinie wird alle 4 Stunden ausgeführt und legt einen Aufbewahrungszeitraum von 1 Woche fest.

Silber
Diese Richtlinie wird täglich ausgeführt und legt einen Aufbewahrungszeitraum von 1 Monat fest.

Bronze
Diese Richtlinie wird täglich ausgeführt und legt einen Aufbewahrungszeitraum von 1 Woche fest.

Um Sicherungsrichtlinien anzuzeigen und zu verwalten und die durch Richtlinien geschützten virtuellen Maschinen und Datenbanken zu überwachen, klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Richtlinienübersicht**.

Wenn Sie eine vorhandene SLA-Richtlinie editieren und die Cloud-Auslagerungsquelle, den Auslagerungszieltyp oder die Optionen des Auslagerungszielservers ändern, wird in zugehörigen Jobs eine vollständige Basissicherung (keine Teilsicherung) während der nächsten Jobausführung gestartet.

Für Installationen von IBM Spectrum Protect Plus Version 10.1.4 ist eine SLA-Demokonfiguration zu Testzwecken verfügbar. Diese Demonstrationsfunktion umfasst die folgenden Elemente:

- Eine Demonstrationssite mit dem Namen **Demo**
- Eine SLA-Richtlinie mit dem Namen **Demo**
- Eine lokale vSnap-Konfiguration für die Demo-SLA

Falls gewünscht, können Sie die Demosite zum Testen von Sicherungs- und Zurückschreibungsoperationen verwenden. Die Daten werden in der lokalen vSnap-Konfiguration gesichert, wenn Sie die SLA-Demorichtlinie ausführen.

Anmerkung: Das integrierte vSnap kann gemäß Definition nur von der Demosite verwendet werden. Sie dürfen das integrierte IBM Spectrum Protect Plus vSnap nicht mit einer anderen Site verwenden.

SLA-Richtlinie erstellen

Sie können angepasste SLA-Richtlinien erstellen, um Richtlinien für Sicherungshäufigkeit, Aufbewahrung, Replikation und Auslagerung zu definieren, die für Ihre Umgebung spezifisch sind.

Informationen zu diesem Vorgang

Wenn eine virtuelle Maschine mehreren SLA-Richtlinien zugeordnet ist, stellen Sie sicher, dass die Richtlinien nicht gleichzeitig ausgeführt werden. Planen Sie die SLA-Richtlinien so, dass zwischen der Ausführung der einzelnen Richtlinien genügend Zeit ist, oder kombinieren Sie die Richtlinien in einer einzigen SLA-Richtlinie.

Wenn eine Momentaufnahmereplikationstask gestartet wird, bevor eine Erstsicherung auf einen vSnap-Server abgeschlossen ist, geben Fehler im Jobprotokoll an, dass für die Datenbank keine Wiederherstellungspunkte vorhanden sind. Führen Sie, nachdem die Erstsicherung auf den vSnap-Server abgeschlos-

© Copyright IBM Corp. 2017, 2019

sen ist, die Replikationstask erneut aus, um die Momentaufnahmen wie in der SLA-Richtlinie konfiguriert zu replizieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine SLA-Richtlinie zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Richtlinienübersicht**.
2. Klicken Sie auf **SLA-Richtlinie hinzufügen**.

   Das Fenster **Neue SLA-Richtlinie** wird angezeigt.
3. Geben Sie in das Feld **Name** einen Namen ein, der eine aussagekräftige Beschreibung der SLA-Richtlinie bereitstellt.
4. Definieren Sie im Abschnitt **Operativer Schutz** unter **Hauptrichtlinie** die folgenden Optionen für Sicherungsoperationen. Diese Operationen werden auf den im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Platte** definierten vSnap-Servern ausgeführt.

   Aufbewahrung
   Geben Sie den Aufbewahrungszeitraum für die Sicherungsmomentaufnahmen an.

   Zeitplan inaktivieren
   Wählen Sie dieses Kontrollkästchen aus, um die Hauptrichtlinie zu erstellen, ohne eine Häufigkeit oder eine Startzeit zu definieren. Richtlinien, die ohne einen Zeitplan erstellt werden, können bedarfsgesteuert ausgeführt werden.

   Häufigkeit
   Geben Sie eine Häufigkeit für Sicherungsoperationen ein.

   Startzeit
   Geben Sie das Datum und die Uhrzeit ein, an dem bzw. zu der die Sicherungsoperation gestartet werden soll.

   Zielsite
   Wählen Sie die Zielsite für die Sicherung zum Sichern von Daten aus.

   Eine Site kann einen oder mehrere vSnap-Server enthalten. Wenn eine Site mehr als einen vSnap-Server enthält, steuert der IBM Spectrum Protect Plus-Server die Datenplatzierung in den vSnap-Servern.

   In dieser Liste werden nur Sites angezeigt, die einem vSnap-Server zugeordnet sind. Sites, die IBM Spectrum Protect Plus hinzugefügt werden, aber keinem vSnap-Server zugeordnet sind, werden nicht angezeigt.

   Nur verschlüsselten Plattenspeicher verwenden
   Wählen Sie dieses Kontrollkästchen aus, um Daten auf verschlüsselten vSnap-Servern zu sichern, wenn Ihre Umgebung eine Kombination aus verschlüsselten und nicht verschlüsselten Servern enthält.

   Einschränkung: Wenn diese Option ausgewählt wird und keine verschlüsselten vSnap-Server verfügbar sind, schlägt der zugeordnete Job fehl.
5. Legen Sie unter **Replikationsrichtlinie** die folgenden Optionen fest, um die asynchrone Replikation von einem vSnap-Server zu einem anderen zu aktivieren. Sie können beispielsweise Daten von der primären Sicherungssite zur sekundären Sicherungssite replizieren.

   Replikationspartnerschaftsanforderung: Diese Optionen gelten für erstellte Replikationspartnerschaften. Informationen zum Hinzufügen einer Replikationspartnerschaft enthalten die Anweisungen in „Replikationspartnerschaft für einen vSnap-Server erstellen” auf Seite 63.

   Sicherungsspeicherreplikation
   Wählen Sie diese Option aus, um die Replikation zu aktivieren.

   Zeitplan inaktivieren
   Wählen Sie dieses Kontrollkästchen aus, um die Replikationsbeziehung zu erstellen, ohne eine Häufigkeit oder eine Startzeit zu definieren.

Häufigkeit
Geben Sie eine Häufigkeit für Replikationsoperationen ein.

Startzeit
Geben Sie das Datum und die Uhrzeit ein, an dem bzw. zu der die Replikationsoperation gestartet werden soll.

Zielsite
Wählen Sie die Zielsite für die Sicherung zum Replizieren von Daten aus.

Eine Site kann einen oder mehrere vSnap-Server enthalten. Wenn eine Site mehr als einen vSnap-Server enthält, steuert der IBM Spectrum Protect Plus-Server die Datenplatzierung in den vSnap-Servern.

In dieser Liste werden nur Sites angezeigt, die einem vSnap-Server zugeordnet sind. Sites, die IBM Spectrum Protect Plus hinzugefügt werden, aber keinem vSnap-Server zugeordnet sind, werden nicht angezeigt.

Nur verschlüsselten Plattenspeicher verwenden
Wählen Sie diese Option aus, um Daten auf verschlüsselte vSnap-Servern zu replizieren, wenn Ihre Umgebung eine Kombination aus verschlüsselten und nicht verschlüsselten Servern enthält.

Einschränkung: Wenn diese Option ausgewählt wird und keine verschlüsselten vSnap-Server verfügbar sind, schlägt der zugeordnete Job fehl.

Dieselbe Aufbewahrung wie bei Quellenauswahl
Wählen Sie diese Option aus, um dieselbe Aufbewahrungsrichtlinie wie für den vSnap-Quellenserver zu verwenden. Um eine andere Aufbewahrungsrichtlinie festzulegen, löschen Sie diese Option und legen Sie eine andere Richtlinie fest.

6. Legen Sie im Abschnitt **Zusätzlicher Schutz** die folgenden Optionen fest, um Daten auszulagern und zu archivieren.

Tipp: Wenn Sie "Zusätzlicher Schutz" angeben, entscheiden Sie sich damit für die Erstellung einer Kopie.

Cloud
Wählen Sie diese Option aus, um Daten in Cloudspeicher oder auf einen Repository-Server auszulagern.

Wichtig: Wenn Sie auf **Zusätzlicher Schutz** > **Cloud** klicken, wird eine inkrementelle Kopie der Daten in einem Cloudspeichersystem oder auf einem IBM Spectrum Protect-Server erstellt.

Daten werden auf dem vSnap-Server für den kurzfristigen Schutz gesichert und dann für den längerfristigen Schutz in den ausgewählten Cloudspeicher oder auf den ausgewählten Repository-Server ausgelagert. Während der ersten Auslagerung eines Sicherungsdatenträgers, wird die Momentaufnahme vollständig gesichert. Nachdem die Auslagerung der Basismomentaufnahme abgeschlossen ist, sind nachfolgende Auslagerungen inkrementell und erfassen kumulative Änderungen, die seit der letzten Auslagerung erfolgt sind. Zurückschreibungsoperationen aus der Cloud oder vom Repository-Server können von jedem verfügbaren vSnap-Server ausgeführt werden.

Zeitplan inaktivieren
Wählen Sie dieses Kontrollkästchen aus, um die Auslagerungsbeziehung zu erstellen, ohne eine Häufigkeit oder eine Startzeit zu definieren.

Häufigkeit
Geben Sie eine Häufigkeit für Auslagerungsoperationen ein.

Startzeit
Geben Sie das Datum und die Uhrzeit ein, an dem bzw. zu der die Auslagerungsoperation gestartet werden soll.

Dieselbe Aufbewahrung wie bei Quellenauswahl
Wählen Sie diese Option aus, um dieselbe Aufbewahrungsrichtlinie für die Auslagerung der Sicherung in die Cloud wie für den vSnap-Quellenserver zu verwenden. Um eine andere Aufbewahrungsrichtlinie festzulegen, löschen Sie diese Option und legen Sie eine andere Richtlinie fest.

Einschränkung: Optionen für die Aufbewahrung von Auslagerungen werden inaktiviert, wenn ein Server, der WORM-Aufbewahrung (WORM = Write Once Read Many) verwendet, im Feld **Auslagerungszielserver** ausgewählt wird.

Quelle
Klicken Sie auf die Quelle für die Auslagerungsoperation:

Hauptrichtlinienziel
Die Quelle der Auslagerungsoperation ist die Zielsite, die im Abschnitt **Hauptrichtlinie** definiert ist.

Replikationsrichtlinienziel
Die Quelle der Auslagerungsoperation ist die Zielsite, die im Abschnitt **Replikationsrichtlinie** definiert ist.

Diese Option ist nur verfügbar, wenn **Sicherungsspeicherreplikation** ausgewählt ist.

Ziel
Klicken Sie auf **Cloud-Server** oder **Repository-Server**.

Ziel
Klicken Sie auf das Cloudspeichersystem oder den Repository-Server, in das bzw. auf den Daten ausgelagert werden sollen.

Diese Liste enthält die sekundären Speichersysteme, die IBM Spectrum Protect Plus hinzugefügt wurden. Wenn kein sekundärer Speicher hinzugefügt wurde oder sekundärer Speicher hinzugefügt werden soll, lesen Sie den Abschnitt „Sekundären Sicherungsspeicher verwalten" auf Seite 269, der Informationen zu unterstützten Cloudspeichersystemen und Repository-Servern enthält und in dem beschrieben ist, wie diese IBM Spectrum Protect Plus hinzugefügt werden.

Archivierung
Wählen Sie diese Option aus, um Daten für den langfristigen Schutz im Cloudspeicher oder auf einem Repository-Server zu archivieren.

Wichtig: Wenn Sie auf **Zusätzlicher Schutz** > **Archivierung** klicken, wird unter Verwendung eines IBM Spectrum Protect-Servers eine vollständige Kopie der Daten in einem Cloudspeichersystem oder auf Band erstellt.

Mit dieser Operation wird eine vollständige Imageauslagerung in den ausgewählten Archivierungsspeicher bereitgestellt.

Zeitplan inaktivieren
Wählen Sie dieses Kontrollkästchen aus, um die Archivierungsbeziehung zu erstellen, ohne eine Häufigkeit oder eine Startzeit zu definieren.

Häufigkeit
Geben Sie eine Häufigkeit für Archivierungsoperationen ein.

Startzeit
Geben Sie das Datum und die Uhrzeit ein, an dem bzw. zu der die Archivierungsoperation gestartet werden soll.

Aufbewahrung
Geben Sie den Aufbewahrungszeitraum für die Archivierungsmomentaufnahmen als Zeiteinheit in Tagen, Monaten oder Jahren an.

Quelle
Klicken Sie auf die Quelle für das Archivierungsziel:

Hauptrichtlinienziel
Die Quelle der Archivierungsoperation ist die Zielsite, die im Abschnitt **Hauptrichtlinie** definiert ist.

Replikationsrichtlinienziel
Die Quelle der Archivierungsoperation ist die Zielsite, die im Abschnitt **Replikationsrichtlinie** definiert ist.

Diese Option ist nur verfügbar, wenn **Sicherungsspeicherreplikation** ausgewählt ist.

Ziel
Klicken Sie auf **Cloud-Server** oder **Repository-Server**.

Ziel
Klicken Sie auf das Cloudspeichersystem oder den Repository-Server, in dem bzw. auf dem Daten archiviert werden sollen.

In dieser Liste werden nur Cloudziele mit einem definierten Archivierungsbucket angezeigt. Um ein Archivierungsbucket für ein Cloudspeichersystem hinzuzufügen, führen Sie die Anweisungen in „Cloudspeicher verwalten" auf Seite 269 aus.

7. Klicken Sie auf **Speichern**. Die SLA-Richtlinie kann jetzt auf Sicherungsjobdefinitionen angewendet werden.

Nächste Schritte

Führen Sie die folgenden Aktionen aus, nachdem eine SLA-Richtlinie erstellt wurde:

Aktion	Vorgehensweise
Ordnen Sie der SLA-Richtlinie Benutzerberechtigungen zu.	Siehe „Rolle erstellen" auf Seite 317.
Erstellen Sie eine Sicherungsjobdefinition, die die SLA-Richtlinie verwendet.	Siehe die Abschnitte zur Sicherung in Kapitel 7, „Hypervisoren schützen", auf Seite 99 und Kapitel 8, „Anwendungen schützen", auf Seite 143.

Zugehörige Konzepte

„Sicherungsspeicherdaten replizieren" auf Seite 5
Wenn Sie die Replikation von Sicherungsdaten aktivieren, werden Daten eines vSnap-Servers auf einem anderen vSnap-Server asynchron repliziert. Sie können beispielsweise Sicherungsdaten eines vSnap-Servers an einer primären Site auf einem vSnap-Server an einer sekundären Site replizieren.

„In sekundären Sicherungsspeicher auslagern" auf Seite 6
Der vSnap-Server ist die primäre Sicherungsposition für Momentaufnahmen. Alle IBM Spectrum Protect Plus-Umgebungen verfügen über mindestens einen vSnap-Server. Wahlweise können Sie Momentaufnahmen aus einem vSnap-Server in sekundären Sicherungsspeicher auslagern.

SLA-Richtlinie editieren

Editieren Sie die Optionen für eine SLA-Richtlinie, um die Änderungen in Ihrer IBM Spectrum Protect Plus-Umgebung widerzuspiegeln.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine SLA-Richtlinie zu editieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Richtlinienübersicht**.
2. Klicken Sie auf das Symbol für Editieren , das einer Richtlinie zugeordnet ist.
   Das Fenster **SLA-Richtlinie editieren** wird angezeigt.
3. Editieren Sie die Richtlinienoptionen und klicken Sie dann auf **Speichern**.

SLA-Richtlinie löschen

Löschen Sie eine SLA-Richtlinie, wenn sie veraltet ist.

Vorbereitende Schritte

Stellen Sie sicher, dass keine Jobs vorhanden sind, die der SLA-Richtlinie zugeordnet sind.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine SLA-Richtlinie zu löschen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Richtlinienübersicht**.
2. Klicken Sie auf das Symbol für Löschen  , das einer SLA-Richtlinie zugeordnet ist.
3. Klicken Sie auf **Ja**, um die Richtlinie zu löschen.
4. Wenn Sie die SLA-Demorichtlinie löschen, rufen Sie **Systemkonfiguration** > **Site** auf und löschen Sie die Site mit dem Namen "Demo".

   Anmerkung:

   Wenn Sie die Demosite löschen, müssen Sie das lokale Host-vSnap mit Benutzerberechtigungsnachweisen bei einer anderen gültigen Site registrieren.

Kapitel 7. Hypervisoren schützen

Sie müssen die Hypervisoren, die in IBM Spectrum Protect Plus geschützt werden sollen, registrieren und anschließend Jobs für die Sicherung und Zurückschreibung der virtuellen Maschinen und Ressourcen, die den Hypervisoren zugeordnet sind, erstellen.

VMware-Daten sichern und zurückschreiben

Damit VMware-Daten geschützt werden, müssen Sie zunächst vCenter Server-Instanzen in IBM Spectrum Protect Plus hinzufügen und dann Jobs für Sicherungs- und Zurückschreibungsoperationen für den Inhalt der Instanzen erstellen.

Systemanforderungen

Stellen Sie sicher, dass Ihre VMware-Umgebung die in „Hypervisoranforderungen” auf Seite 23 beschriebenen Systemanforderungen erfüllt.

Unterstützung für VMware-Tags

IBM Spectrum Protect Plus unterstützt Tags virtueller VMware-Maschinen. Tags werden in vSphere angewendet und gestatten es, dass Benutzer virtuellen Maschinen Metadaten zuordnen können. Werden VM-Tags in vSphere angewendet und dem IBM Spectrum Protect Plus-Bestand hinzugefügt, können sie über den Filter **Anzeigen** > **Tags & Kategorien** angezeigt werden, wenn Sie eine Jobdefinition erstellen. Weitere Informationen zum VMware-Tagging finden Sie in Kennzeichnen von Objekten.

Verschlüsselungsunterstützung

Die Sicherung und Zurückschreibung verschlüsselter virtueller Maschinen wird in Umgebungen mit vSphere 6.5 und höher unterstützt. Verschlüsselte virtuelle Maschinen können auf der Ebene virtueller Maschinen an ihrer ursprünglichen Position gesichert und zurückgeschrieben werden. Wenn Sie an einer alternativen Position zurückschreiben, wird die virtuelle Maschine ohne Verschlüsselung zurückgeschrieben und sie muss nach Beendigung der Zurückschreibung über vCenter Server manuell verschlüsselt werden.

Folgende vCenter Server-Berechtigungen sind erforderlich, damit Operationen für verschlüsselte virtuelle Maschinen möglich sind:

- Cryptographer.Access
- Cryptographer.AddDisk
- Cryptographer.Clone

vCenter Server-Instanz hinzufügen

Wenn IBM Spectrum Protect Plus eine vCenter Server-Instanz hinzugefügt wird, wird ein Bestand der Instanz erfasst, der es Ihnen ermöglicht, Sicherungs- und Zurückschreibungsjobs auszuführen und Berichte zu erstellen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine vCenter Server-Instanz hinzuzufügen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **VMware**.
2. Klicken Sie auf **vCenter verwalten**.
3. Klicken Sie auf **vCenter hinzufügen**.
4. Füllen Sie die Felder im Abschnitt **vCenter-Eigenschaften** aus:

© Copyright IBM Corp. 2017, 2019

Hostname/IP
Geben Sie die auflösbare IP-Adresse oder einen auflösbaren Pfad und Maschinennamen ein.

Vorhandenen Benutzer verwenden
Aktivieren Sie dieses Feld, um einen zuvor eingegebenen Benutzernamen und ein zuvor eingegebenes Kennwort für die vCenter Server-Instanz auszuwählen.

Benutzername
Geben Sie Ihren Benutzernamen für die vCenter Server-Instanz ein.

Kennwort
Geben Sie Ihr Kennwort für die vCenter Server-Instanz ein.

Port
Geben Sie den Kommunikationsport der vCenter Server-Instanz ein. Wählen Sie das Kontrollkästchen **SSL verwenden** aus, um eine verschlüsselte Secure Sockets Layer-Verbindung (SSL-Verbindung) zu aktivieren. Der Standardport ist 80 für Nicht-SSL-Verbindungen und 443 für SSL-Verbindungen.

5. Konfigurieren Sie im Abschnitt **Optionen** die folgende Option:

   Maximale Anzahl VMs, die pro ESX-Server und pro SLA gleichzeitig verarbeitet werden sollen
   Definieren Sie die maximale Anzahl der VM-Momentaufnahmen, die auf dem ESX-Server gleichzeitig verarbeitet werden sollen.
6. Klicken Sie auf **Speichern**. IBM Spectrum Protect Plus bestätigt eine Netzverbindung, fügt die vCenter Server-Instanz zur Datenbank hinzu und katalogisiert dann die Instanz.

   Wird eine Nachricht angezeigt, die angibt, dass die Verbindung nicht erfolgreich ist, überprüfen Sie Ihre Eingaben. Sind Ihre Eingaben korrekt und ist die Verbindung nicht erfolgreich, bitten Sie einen Netzadministrator, die Verbindungen zu überprüfen.

Nächste Schritte
Führen Sie die folgende Aktion aus, nachdem Sie eine vCenter Server-Instanz hinzugefügt haben:

Aktion	Vorgehensweise
Fügen Sie dem Hypervisor Benutzerberechtigungen hinzu.	Siehe „Rolle erstellen” auf Seite 317.

Zugehörige Konzepte
„Identitäten verwalten” auf Seite 322
Bei einigen Funktionen in IBM Spectrum Protect Plus sind Berechtigungsnachweise für den Zugriff auf Ihre Ressourcen erforderlich. Beispielsweise stellt IBM Spectrum Protect Plus eine Verbindung zu Oracle-Servern als der lokale Betriebssystembenutzer her, der während der Registrierung angegeben wird, um Tasks wie Katalogisierung, Datenschutz und Datenzurückschreibung auszuführen.

Zugehörige Tasks
„VMware-Daten sichern” auf Seite 107
Verwenden Sie einen Sicherungsjob, um VMware-Ressourcen, wie z. B. virtuelle Maschinen, Datenspeicher, Ordner, vApps und Datencenter, mit Momentaufnahmen zu sichern.

„VMware-Daten zurückschreiben” auf Seite 116
VMware-Zurückschreibungsjobs unterstützen Instant VM Restore- und Instant Disk Restore-Szenarios, die automatisch auf der Basis der ausgewählten Quelle erstellt werden.

Berechtigungen für virtuelle Maschinen
Für die virtuellen Maschinen, die einem VMware-Provider zugeordnet sind, sind vCenter Server-Berechtigungen erforderlich. Diese Berechtigungen sind in der vCenter-Administratorrolle enthalten.

Verfügt der Benutzer, der dem Provider zugeordnet ist, nicht über die Administratorrolle für ein Bestandsobjekt, muss er einer Rolle zugeordnet werden, die über die folgenden erforderlichen Berechtigungen verfügt. Stellen Sie sicher, dass Berechtigungen an untergeordnete Objekte weitergegeben werden. Anweisungen finden Sie in der VMware-Dokumentation über das Hinzufügen einer Berechtigung zu einem Bestandsobjekt.

vCenter Server-Objekt	Erforderliche Berechtigungen
Alarm	• Alarm bestätigen • Alarmstatus festlegen
Verschlüsselungsoperationen	• Platten hinzufügen • Direktzugriff • Verschlüsseln • Neu verschlüsseln • Verschlüsselungsrichtlinien verwalten
Datencenter	• Datencenter erstellen • Datencenter rekonfigurieren
Datenspeicher	• Speicherbereich zuordnen • Datenspeicher durchsuchen • Datenspeicher konfigurieren • Dateioperationen auf unterer Ebene • Datei entfernen • Dateien der virtuellen Maschine aktualisieren
Datenspeichercluster	• Datenspeichercluster konfigurieren
Distributed Switch	• Erstellen • Löschen • Hostoperation • Ändern • Verschieben • Netz-E/A-Steuerungsoperation • Richtlinienoperation • Portkonfigurationsoption • Porteinstellungsoperation • VSPAN-Operation
ESX Agent Manager	• Konfigurieren • Ändern • Anzeigen
Erweiterung	• Erweiterung registrieren
Ordner	• Ordner erstellen • Ordner löschen • Ordner verschieben • Ordner umbenennen

vCenter Server-Objekt	Erforderliche Berechtigungen
Global	• Task abbrechen • Diagnose (für Fehlerbehebung, nicht erforderlich für Operationen) • Methoden inaktivieren • Methoden aktivieren • Lizenzen • Ereignis protokollieren • Angepasste Attribute verwalten • Angepasste Attribute definieren • Einstellungen
Host > Konfiguration	• Erweiterte Einstellungen • Speicherpartitionskonfiguration
Bestandsservice > vSphere-Tagging	• vSphere-Tag zuordnen oder Zuordnung aufheben • vSphere-Tag erstellen • vSphere-Tag-Kategorie erstellen • UsedBy-Feld für Kategorie ändern • UsedBy-Feld für Tag ändern
Netz	• Netz zuordnen • Konfigurieren • Netz verschieben • Entfernen
Ressource	• Empfehlung anwenden • vApp Ressourcenpool zuordnen • Virtuelle Maschine Ressourcenpool zuordnen • Ressourcenpool erstellen • Ausgeschaltete VM migrieren • Eingeschaltete VM migrieren • Ressourcenpool ändern • Ressourcenpool verschieben • vMotion abfragen • Ressourcenpool entfernen • Ressourcenpool umbenennen
Sitzungen	• Sitzungen anzeigen und stoppen
Speichersichten	• Service konfigurieren • Anzeigen
Tasks	• Task erstellen • Task aktualisieren

vCenter Server-Objekt	Erforderliche Berechtigungen
Virtuelle Maschine > Konfiguration	• Vorhandene Platte hinzufügen • Neue Platte hinzufügen • Einheit hinzufügen oder entfernen • Erweitert • CPU-Zahl ändern • Ressource ändern • managedBy konfigurieren • Plattenänderungen überwachen • Plattenlease • Verbindungseinstellungen anzeigen • Virtuelle Platte erweitern • Host-USB-Einheit • Speicher • Einheiteneinstellungen ändern • Fehlertoleranzkompatibilität abfragen • Dateien ohne Eigner abfragen • Roheinheit • Aus Pfad erneut laden • Platte entfernen (Zuordnung der virtuellen Platte aufheben und virtuelle Platte entfernen) • Umbenennen • Gastinformationen zurücksetzen • Anmerkung festlegen • Einstellungen • Position der Auslagerungsdatei • Virtuelle Maschine entsperren • VM-Kompatibilität aktualisieren
Virtuelle Maschine > Gastoperationen	• Gastoperationsänderungen • Programmausführung der Gastoperation • Gastoperationsabfragen

vCenter Server-Objekt	Erforderliche Berechtigungen
Virtuelle Maschine > Interaktion	• Frage beantworten • Sicherungsoperation auf virtueller Maschine • CD-Datenträger konfigurieren • Diskette konfigurieren • Konsoleninteraktion • Screenshot erstellen • Alle Platten defragmentieren • Einheitenverbindung • Fehlertoleranz inaktivieren • Fehlertoleranz aktivieren • Management des Gastbetriebssystems durch VIX API • USB HID-Scancodes einfügen • Zurücksetzungs- oder Verkleinerungsoperationen ausführen • Ausschalten • Einschalten • Aufzeichnungssitzung in VM • Wiedergabesitzung in VM • Zurücksetzen • Fehlertoleranz fortsetzen • Aussetzen • Fehlertoleranz aussetzen • Failover testen • Neustart sekundärer VM testen • Fehlertoleranz ausschalten • Fehlertoleranz einschalten • VMware Tools installieren
Virtuelle Maschine > Bestand	• Aus vorhandener erstellen • Neu erstellen • Verschieben • Registrieren • Entfernen • Registrierung zurücknehmen

vCenter Server-Objekt	Erforderliche Berechtigungen
Virtuelle Maschine > Bereitstellung	• Festplattenzugriff zulassen • Lesezugriff auf Festplatte zulassen • Download virtueller Maschinen zulassen • Upload von Dateien virtueller Maschinen zulassen • Schablone klonen • Virtuelle Maschine klonen • Schablone aus virtueller Maschine erstellen • Anpassen • Schablone implementieren • Als Schablone markieren • Als virtuelle Maschine markieren • Anpassungsspezifikation ändern • Festplatten heraufstufen • Anpassungsspezifikationen lesen
Virtuelle Maschine > Servicekonfiguration	• Benachrichtigungen zulassen • Abrufen globaler Ereignisbenachrichtigungen zulassen • Servicekonfigurationen verwalten • Servicekonfigurationen ändern • Servicekonfigurationen abfragen • Servicekonfigurationen lesen
Virtuelle Maschine > Momentaufnahmeverwaltung	• Momentaufnahme erstellen • Momentaufnahme entfernen • Momentaufnahme umbenennen • Momentaufnahme wiederherstellen
Virtuelle Maschine > vSphere Replication	• Replikation konfigurieren • Replikation verwalten • Replikation überwachen

vCenter Server-Objekt	Erforderliche Berechtigungen
vApp	• VM zu vApp hinzufügen • Ressourcenpool vApp zuordnen • vApp anderer vApp zuordnen • Klonen • Erstellen • Löschen • Exportieren • Importieren • Verschieben • Ausschalten • Einschalten • Umbenennen • Aussetzen • Registrierung zurücknehmen • OVF-Umgebung anzeigen • vApp-Anwendungskonfiguration • vApp-Instanzkonfiguration • vApp-managedBy-Konfiguration • vApp-Ressourcenkonfiguration

VMware-Ressourcen erkennen
VMware-Ressourcen werden automatisch erkannt, nachdem die vCenter Server-Instanz IBM Spectrum Protect Plus hinzugefügt wurde. Sie können jedoch einen Bestandsjob ausführen, um alle Änderungen zu finden, die seit dem Hinzufügen der Instanz aufgetreten sind.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Bestandsjob auszuführen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **VMware**.
2. Wählen Sie in der Liste der vCenter Server-Instanzen eine Instanz aus oder klicken Sie auf den Link für die Instanz, um zu der gewünschten Ressource zu navigieren. Wenn beispielsweise ein Bestandsjob für eine einzelne virtuelle Maschine in der Instanz ausgeführt werden soll, klicken Sie auf den Instanz-link und wählen Sie dann eine virtuelle Maschine aus.
3. Klicken Sie auf **Bestandsverarbeitung ausführen**.

Verbindung zu einer virtuellen Maschine des vCenter-Servers testen
Sie können die Verbindung zu einer virtuellen Maschine des vCenter-Servers testen. Die Testfunktion verifiziert die Kommunikation mit der virtuellen Maschine und testet DNS-Einstellungen zwischen der virtuellen IBM Spectrum Protect-Appliance und der virtuellen Maschine.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Verbindung zu testen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **VMware**.
2. Klicken Sie in der Liste der vCenter Server-Instanzen auf den Link für einen vCenter-Server, um zu den einzelnen virtuellen Maschinen zu navigieren.
3. Wählen Sie eine virtuelle Maschine aus und klicken Sie dann auf **Optionen auswählen**.
4. Wählen Sie **Vorhandenen Benutzer verwenden** aus.

5. Wählen Sie in der Liste **Benutzer auswählen** einen Benutzer aus.
6. Klicken Sie auf **Testen**.

VMware-Daten sichern

Verwenden Sie einen Sicherungsjob, um VMware-Ressourcen, wie z. B. virtuelle Maschinen, Datenspeicher, Ordner, vApps und Datencenter, mit Momentaufnahmen zu sichern.

Vorbereitende Schritte

Lesen Sie die folgenden Prozeduren und Hinweise, bevor Sie eine Sicherungsjobdefinition erstellen:

- Registrieren Sie die Provider, die gesichert werden sollen. Weitere Informationen finden Sie in „vCenter Server-Instanz hinzufügen" auf Seite 99.
- Konfigurieren Sie SLA-Richtlinien. Weitere Informationen finden Sie in „Sicherungsrichtlinien erstellen" auf Seite 75.
- Bevor ein IBM Spectrum Protect Plus-Benutzer Sicherungs- und Zurückschreibungsoperationen implementieren kann, müssen dem Benutzer Rollen zugeordnet werden. Erteilen Sie Benutzern mithilfe des Fensters **Accounts** Zugriff auf Hypervisoren und Sicherungs- und Zurückschreibungsoperationen. Rollen und zugehörige Berechtigungen werden während der Benutzeraccounterstellung zugeordnet. Weitere Informationen finden Sie in Kapitel 13, „Benutzerzugriff verwalten", auf Seite 311 und „Benutzeraccounts verwalten" auf Seite 320.
- Wenn eine virtuelle Maschine mehreren SLA-Richtlinien zugeordnet ist, stellen Sie sicher, dass die Richtlinien nicht gleichzeitig ausgeführt werden. Planen Sie die SLA-Richtlinien so, dass zwischen der Ausführung der einzelnen Richtlinien genügend Zeit ist, oder kombinieren Sie die Richtlinien in einer einzigen SLA-Richtlinie.
- Wenn Ihr vCenter eine virtuelle Maschine ist, sollte sich das vCenter in einem dedizierten Datenspeicher befinden und das vCenter in einem separaten Sicherungsjob gesichert werden, um den Datenschutz zu maximieren.
- Beim Sichern von virtuellen VMware-Maschinen lädt IBM Spectrum Protect Plus Dateien mit der Erweiterung .vmx, .vmxf und .nvram herunter (falls erforderlich) und überträgt dann diese Dateien bei Bedarf auf den vSnap-Server. Damit diese Operation erfolgreich ausgeführt werden kann, muss die IBM Spectrum Protect Plus-Appliance alle geschützten ESXi-Hosts auflösen und auf diese Hosts zugreifen können. Bei der Kommunikation mit einem ESXi-Host muss die korrekte IP-Adresse zurückgegeben werden.
- Wenn eine VM durch eine SLA-Richtlinie geschützt wird, werden die Sicherungen der VM abhängig von den Aufbewahrungsparametern der SLA-Richtlinie selbst dann beibehalten, wenn die VM aus vCenter entfernt wird.
- In einigen Fällen schlagen VMware-Sicherungsjobs mit dem Fehler "Bereitstellung fehlgeschlagen" fehl. Um dieses Problem zu beheben, erhöhen Sie die maximale Anzahl NFS-Mounts auf mindestens 64, indem Sie die Werte NFS.MaxVolumes (vSphere 5.5 und höher) und NFS41.MaxVolumes (vSphere 6.0 und höher) verwenden. Führen Sie die Anweisungen in Increasing the default value that defines the maximum number of NFS mounts on an ESXi/ESX host aus.
- Wenn für eine vorhandene VM die Funktion vMotion ausgeführt wurde, führt IBM Spectrum Protect Plus, falls erforderlich, eine Aktualisierung mit Referenzversionen aus.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen VMware-Sicherungsjob zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **VMware**.
2. Wählen Sie Ressourcen aus, die gesichert werden sollen.

   Verwenden Sie die Suchfunktion, um nach verfügbaren Ressourcen zu suchen, und wechseln Sie mithilfe des Filters **Sicht** zwischen den angezeigten Ressourcen. Verfügbare Optionen sind **VMs und Schablonen**, **VMs**, **Datenspeicher**, **Tags und Kategorien** und **Hosts und Cluster**. Tags werden in vSphere angewendet. Sie ermöglichen es einem Benutzer, virtuellen Maschinen Metadaten zuzuordnen.

3. Klicken Sie auf **SLA-Richtlinie auswählen**, um eine oder mehrere SLA-Richtlinien, die Ihre Sicherungsdatenkriterien erfüllen, zur Jobdefinition hinzuzufügen.
4. Um die Jobdefinition mithilfe von Standardoptionen zu erstellen, klicken Sie auf **Speichern**.

   Der Job wird wie mit den von Ihnen ausgewählten SLA-Richtlinien definiert ausgeführt. Um den Job manuell auszuführen, klicken Sie auf **Jobs und Operationen** > **Zeitplan**. Wählen Sie den Job aus und klicken Sie auf **Aktionen** > **Starten**.

   Tipp: Die Schaltfläche **Ausführen** ist nur für die Sicherung eines einzelnen Hypervisors aktiviert; auf den Hypervisor muss außerdem eine SLA-Richtlinie angewendet sein.

   Wenn die Jobdefinition gespeichert wird, werden verfügbare Platten virtueller Maschinen (VMDKs) in einer virtuellen Maschine erkannt und angezeigt, wenn **VMs und Schablonen** im Filter **Sicht** ausgewählt wird. Standardmäßig werden diese VMDKs derselben SLA-Richtlinie wie die virtuelle Maschine zugeordnet. Wenn Sie eine differenziertere Sicherungsoperation wünschen, können Sie einzelne VMDKs aus der SLA-Richtlinie ausschließen. Anweisungen finden Sie in „VMDKs aus der SLA-Richtlinie für einen Job ausschließen” auf Seite 111.
5. Um Optionen zu editieren, bevor die Jobdefinition erstellt wird, klicken Sie auf **Optionen auswählen**.

   Definieren Sie im Abschnitt **Sicherungsoptionen** die folgenden Jobdefinitionsoptionen:

   Schreibgeschützte Datenspeicher überspringen

   Mit dieser Option werden Datenspeicher übersprungen, die als schreibgeschützt bereitgestellt werden.

   Temporäre Datenspeicher überspringen, die für Instant Access bereitgestellt werden

   Mit dieser Option werden temporäre Instant Access-Datenspeicher aus der Sicherungsjobdefinition ausgeschlossen.

   VADP-Proxy

   Wählen Sie einen VADP-Proxy aus, um die Last auszugleichen.

   Priorität

   Definieren Sie die Sicherungspriorität der ausgewählten Ressource. Ressourcen mit einer höheren Priorität werden in dem Job zuerst gesichert. Klicken Sie im Abschnitt **VMware-Sicherung** auf die Ressource, der eine Priorität zugeordnet werden soll, und definieren Sie dann die Sicherungspriorität im Feld **Priorität**. Definieren Sie 1 für die Ressource mit der höchsten Priorität oder 10 für die Ressource mit der geringsten Priorität. Wird kein Prioritätswert definiert, wird automatisch der Standardwert 5 zugeordnet.

   Definieren Sie im Abschnitt **Momentaufnahmeoptionen** die folgenden Jobdefinitionsoptionen:

   VM-Momentaufnahmeanwendung/Dateisystem konsistent machen

   Aktivieren Sie diese Option, um die Anwendungs- oder Dateisystemkonsistenz für die VM-Momentaufnahme zu aktivieren. Alle VSS-konformen Anwendungen, wie z. B. Microsoft Active Directory, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL, und der Systemstatus werden stillgelegt. VMDKs und virtuelle Maschinen können sofort bereitgestellt werden, um Daten zurückzuschreiben, die sich auf die stillgelegten Anwendungen beziehen.

   Wiederholungsversuche für VM-Momentaufnahme

   Definieren Sie, wie oft IBM Spectrum Protect Plus versuchen soll, eine anwendungs- oder dateikonsistente Momentaufnahme einer virtuellen Maschine zu erfassen, bevor der Job abgebrochen wird. Wenn die Option **Auf nicht stillgelegte Momentaufnahme zurückgreifen, wenn die stillgelegte Momentaufnahme fehlschlägt** aktiviert wird, wird eine nicht stillgelegte Momentaufnahme nach den Wiederholungsversuchen erstellt.

   Auf nicht stillgelegte Momentaufnahme zurückgreifen, wenn die stillgelegte Momentaufnahme fehlschlägt

   Aktivieren Sie diese Option, um auf eine Momentaufnahme zurückzugreifen, die nicht anwendungs- oder dateisystemkonsistent ist, wenn die anwendungskonsistente Momentaufnahme fehlschlägt. Mit der Auswahl dieser Option wird sichergestellt, dass eine nicht stillgelegte Momentaufnahme erstellt

wird, wenn Umgebungsprobleme die Erfassung einer anwendungs- oder dateisystemkonsistenten Momentaufnahme verhindern.

Definieren Sie im Abschnitt **Agentenoptionen** die folgenden Jobdefinitionsoptionen:

SQL-Protokolle abschneiden

Um Anwendungsprotokolle für SQL Server während des Sicherungsjobs abzuschneiden, aktivieren Sie die Option **SQL-Protokolle abschneiden**. Die Berechtigungsnachweise für die zugeordnete virtuelle Maschine müssen mithilfe der Optionen "Benutzername für Gastbetriebssystem" und "Kennwort für Gastbetriebssystem" in der Sicherungsjobdefinition erstellt werden. Wenn die virtuelle Maschine einer Domäne zugeordnet ist, folgt die Benutzeridentität dem Standardformat *Domäne\Name*. Ist der Benutzer ein lokaler Administrator, wird das Format *lokaler_Administrator* verwendet.

Die Benutzeridentität muss über Berechtigungen für den lokalen Administrator verfügen. Auf dem SQL Server-Server muss der Systemanmeldeberechtigungsnachweis über die folgenden Berechtigungen verfügen:

- SQL Server-Berechtigungen "sysadmin" müssen aktiviert werden.
- Das Recht **Als Service anmelden** muss definiert werden. Weitere Informationen zu diesem Recht finden Sie in Add the Log on as a service Right to an Account.

IBM Spectrum Protect Plus generiert Protokolldateien für die Protokollabschneidefunktion und kopiert sie an die folgende Position auf der IBM Spectrum Protect-Appliance:

```
/data/log/guestdeployer/spätestes_Datum/letzter_Eintrag/VM-Name
```

Dabei sind: *spätestes_Datum* ist das Datum, an dem der Sicherungsjob und die Protokollabschneidung ausgeführt wurden. *letzter_Eintrag* ist die UUID (Universal Unique Identifier) für den Job und *VM-Name* ist der Hostname oder die IP-Adresse der VM, auf der die Protokollabschneidung stattgefunden hat.

Einschränkung: Die Dateiindexierung und Dateizurückschreibung werden nicht von Zurückschreibungspunkten unterstützt, die in Cloudressourcen oder auf Repository-Server ausgelagert wurden.

Dateimetadaten katalogisieren

Aktivieren Sie die Dateiindexierung für die zugeordnete Momentaufnahme. Wenn die Dateiindexierung abgeschlossen ist, können einzelne Dateien mithilfe des Fensters **Dateizurückschreibung** in IBM Spectrum Protect Plus zurückgeschrieben werden. Berechtigungsnachweise für die zugeordnete virtuelle Maschine müssen mithilfe eines SSH-Schlüssels oder der Optionen **Benutzername für Gastbetriebssystem** und **Kennwort für Gastbetriebssystem** in der Sicherungsjobdefinition erstellt werden. Stellen Sie sicher, dass von der IBM Spectrum Protect Plus-Appliance entweder mithilfe eines DNS oder Hostnamens auf die virtuelle Maschine zugegriffen werden kann.

Einschränkungen: SSH-Schlüssel sind kein gültiger Berechtigungsmechanismus für Windows-Plattformen.

Die Dateiindexierung und Dateizurückschreibung werden nicht von Zurückschreibungspunkten unterstützt, die in Cloudressourcen oder auf Repository-Server ausgelagert wurden.

Dateien ausschließen

Geben Sie Verzeichnisse ein, die übersprungen werden sollen, wenn die Dateiindexierung ausgeführt wird. Dateien in diesen Verzeichnissen werden nicht dem IBM Spectrum Protect Plus-Katalog hinzugefügt und sind für die Dateiwiederherstellung nicht verfügbar. Verzeichnisse können mit einer exakten Übereinstimmung oder mit Sternen als Platzhalterzeichen, die vor dem Muster (*test) oder hinter dem Muster (test*) angegeben werden, ausgeschlossen werden. Mehrere Sterne als Platzhalterzeichen werden auch in einem einzelnen Muster unterstützt. Die Muster unterstützen alphanumerische Standardzeichen sowie die folgenden Sonderzeichen: - _ und *. Trennen Sie mehrere Filter durch ein Semikolon voneinander.

Vorhandenen Benutzer verwenden

Wählen Sie einen zuvor eingegebenen Benutzernamen und ein zuvor eingegebenes Kennwort für den Provider aus.

Benutzername/Kennwort für Gastbetriebssystem

Für einige Tasks (wie z. B. Katalogisierung von Dateimetadaten, Dateizurückschreibung und IP-Rekonfiguration) müssen für die zugeordnete virtuelle Maschine Berechtigungsnachweise erstellt werden. Geben Sie den Benutzernamen und das Kennwort ein und stellen Sie sicher, dass von der IBM Spectrum Protect Plus-Appliance entweder mithilfe eines DNS oder Hostnamens auf die virtuelle Maschine zugegriffen werden kann.

6. Um nach Fehlern bei einer Verbindung zu einer virtuellen Hypervisormaschine zu suchen, verwenden Sie die Funktion **Test**.

   Die Funktion **Test** verifiziert die Kommunikation mit der virtuellen Maschine und testet DNS-Einstellungen zwischen der IBM Spectrum Protect Plus-Appliance und der virtuellen Maschine. Um eine Verbindung zu testen, wählen Sie eine einzelne virtuelle Maschine aus und klicken Sie dann auf **Optionen auswählen**. Wählen Sie **Vorhandenen Benutzer verwenden** aus und wählen Sie einen zuvor eingegebenen Benutzernamen und ein zuvor eingegebenes Kennwort für die Ressource aus. Die Schaltfläche zum **Testen** wird rechts neben der Schaltfläche **Speichern** im Abschnitt **Optionen** angezeigt. Klicken Sie auf die Schaltfläche zum **Testen**.
7. Klicken Sie auf **Speichern**.
8. Um zusätzliche Optionen zu konfigurieren, klicken Sie auf das Feld **Richtlinienoptionen**, das dem Job im Abschnitt **SLA-Richtlinienstatus** zugeordnet ist. Definieren Sie die zusätzlichen Richtlinienoptionen:

   Vorscripts und Nachscripts

   Führen Sie ein Vorscript oder Nachscript aus. Vorscripts und Nachscripts sind Scripts, die vor oder nach der Ausführung eines Jobs ausgeführt werden können. Windows-basierte Maschinen unterstützen Batch- und PowerShell-Scripts, während Linux-basierte Maschinen Shell-Scripts unterstützen.

   Wählen Sie im Abschnitt **Vorscript** oder **Nachscript** ein hochgeladenes Script und einen Scriptserver aus, auf dem das Script ausgeführt wird. Scripts und Scriptserver werden auf der Seite **Systemkonfiguration** > **Script** konfiguriert.

   Um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt, wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus.

   Wenn diese Option aktiviert wird und ein Vorscript oder Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird versucht, die Sicherungs- oder Zurückschreibungsoperation auszuführen, und der Taskstatus für das Vorscript wird als ABGESCHLOSSEN zurückgemeldet. Wenn ein Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird der Taskstatus für das Nachscript als ABGESCHLOSSEN zurückgemeldet.

   Wenn diese Option inaktiviert wird, wird nicht versucht, die Sicherung oder Zurückschreibung auszuführen, und der Taskstatus für das Vorscript oder Nachscript wird als FEHLGESCHLAGEN zurückgemeldet.

   Bestandsverarbeitung vor Sicherung ausführen

   Führen Sie einen Bestandsjob aus und erfassen Sie die neuesten Daten der ausgewählten Ressourcen, bevor Sie den Sicherungsjob starten.

   Ressourcen ausschließen

   Schließen Sie bestimmte Ressourcen mit einzelnen oder mehreren Ausschlussmustern aus dem Sicherungsjob aus. Ressourcen können mit einer exakten Übereinstimmung oder mit Sternen als Platzhalterzeichen, die vor dem Muster (*test) oder hinter dem Muster (test*) angegeben werden, ausgeschlossen werden.

   Mehrere Sterne als Platzhalterzeichen werden auch in einem einzelnen Muster unterstützt. Die Muster unterstützen alphanumerische Standardzeichen sowie die folgenden Sonderzeichen: - _ und *.

   Trennen Sie mehrere Filter durch ein Semikolon voneinander.

   Gesamtsicherung der Ressourcen erzwingen

Erzwingen Sie Basissicherungsoperationen für bestimmte virtuelle Maschinen oder Datenbanken in der Sicherungsjobdefinition. Trennen Sie mehrere Ressourcen durch ein Semikolon voneinander.

9. Um alle zusätzlichen Optionen zu speichern, die konfiguriert wurden, klicken Sie auf **Speichern**.

Nächste Schritte

Sie können die folgenden Aktionen ausführen, nachdem Sie einen Sicherungsjob definiert haben:

Aktion	Vorgehensweise
Wenn Sie eine Linux-Umgebung verwenden, ziehen Sie die Erstellung von VADP-Proxys in Betracht, um eine Lastverteilung zu ermöglichen.	Siehe „VADP-Proxys erstellen” auf Seite 113.
Erstellen Sie eine VMware-Zurückschreibungsjob-definition.	Siehe „VMware-Daten zurückschreiben” auf Seite 116.

Zugehörige Konzepte

„Scripts für Sicherungs- und Zurückschreibungsoperationen konfigurieren” auf Seite 267
Vorscripts und Nachscripts sind Scripts, die ausgeführt werden können, bevor oder nachdem Sicherungs- und Zurückschreibungsjobs auf Jobebene ausgeführt werden. Unterstützt werden Shell-Scripts für Linux-basierte Systeme sowie Batch- und PowerShell-Scripts für Windows-basierte Systeme. Scripts werden lokal erstellt, über die Seite **Script** in Ihre Umgebung hochgeladen und dann auf Jobdefinitionen angewendet.

Zugehörige Tasks

„Jobs starten” auf Seite 264
Sie können einen Job selbst dann bedarfsgesteuert ausführen, wenn die Ausführung des Jobs gemäß einem Zeitplan festgelegt ist.

VMDKs aus der SLA-Richtlinie für einen Job ausschließen

Nachdem Sie eine Sicherungsjobdefinition gespeichert haben, können Sie einzelne VMDKs in einer virtuellen Maschine aus der SLA-Richtlinie ausschließen, die dem Job zugeordnet ist.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um VMDKs aus der SLA-Richtlinie auszuschließen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **VMware**.
2. Wählen Sie **VMs und Schablonen** im Filter **Sicht** aus.
3. Klicken Sie auf den Link für das vCenter und klicken Sie dann auf den Link für die virtuelle Maschine, die die auszuschließenden VMDKs enthält.
4. Wählen Sie eine oder mehrere VMDKs aus und klicken Sie dann auf **SLA-Richtlinie auswählen**.
5. Wählen Sie das Kontrollkästchen für die ausgewählte SLA-Richtlinie ab und klicken Sie dann auf **Speichern**.

Linux-basierte vCenter Server-Appliance sichern

Um eine Linux-basierte vCenter Server-Appliance sichern zu können, müssen Sie die VMware-Scripts "pre-freeze-script" und "post-thaw script" in der virtuellen vCenter-Maschine ändern, um beschädigte vCenter-Sicherungen zu verhindern.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Scripts zu ändern:

1. Navigieren auf der virtuellen Maschine zum Verzeichnis `/usr/sbin` und ersetzen Sie den Inhalt des Scripts `pre-freeze-script` durch den folgenden Inhalt:

```
#!/bin/bash
#set log directory
log="/var/log/vpostgres_backup.log"
#set and log start date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Start of creation consistent state" >> ${log}
```

```
#execute freeze command
cmd="echo \"SELECT pg_start_backup('${today}', true);\" | sudo /opt/vmware/vpostgres/9.4/bin/psql -U postgres >> ${log}
2>&1"
eval ${cmd}
#set and log end date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Finished freeze script" >> ${log}
```

2. Ersetzen Sie den Inhalt des Scripts `post-thaw-script` durch den folgenden Inhalt:

```
#!/bin/bash
#set log directory
log="/var/log/vpostgres_backup.log"
#set and log start date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Release of backup" >> ${log}
#execute release command
cmd="echo \"SELECT pg_stop_backup();\" | sudo /opt/vmware/vpostgres/9.4/bin/psql -U postgres >> ${log} 2>&1"
eval ${cmd}
#set and log end date
today=`date +%Y\/%m\/%d\ %H:%M:%S`
echo "${today}: Finished thaw script" >> ${log}
```

VADP-Sicherungsproxys verwalten

In IBM Spectrum Protect Plus können Sie Proxys für die Ausführung von VMware-Sicherungsjobs mithilfe von vStorage API for Data Protection (VADP) in Linux-Umgebungen erstellen. Die Proxys verringern den Bedarf an Systemressourcen durch die Aktivierung der Lastverteilung und des Lastausgleichs. Drosselung stellt sicher, dass mehrere VADP-Proxys optimal genutzt werden, um den Datendurchsatz zu maximieren. Bei jeder virtuellen Maschine, die gesichert werden soll, stellt IBM Spectrum Protect Plus fest, welcher VADP-Proxy am wenigsten ausgelastet ist und über den größten verfügbaren Speicher und die meisten freien Tasks verfügt. Freie Tasks werden durch die Anzahl verfügbarer CPU-Kerne oder mit der Option **Softcap-Task-Limit** bestimmt.

Stellen Sie sicher, dass Sie über die erforderlichen Benutzerberechtigungen für die Arbeit mit VADP-Proxys verfügen. Anweisungen zur Verwaltung von Berechtigungen für VADP-Proxys finden Sie in „Berechtigungstypen” auf Seite 317.

Die Sicherung einer virtuellen VMware-Maschine umfasst die folgenden Dateien:

- Allen Platten entsprechende VMDKs. Bei der Basissicherung werden alle zugeordneten Daten erfasst oder alle Daten, wenn sich Platten in NFS-Datenspeichern befinden. Bei Teilsicherungen werden nur die Blöcke erfasst, die sich seit der letzten erfolgreichen Sicherung geändert haben.
- VM-Schablonen
- VMware-Dateien mit folgenden Erweiterungen:
  - .vmx
  - .vmfx (falls verfügbar)
  - .nvram (Speicherung des Status des VM-BIOS)

Sind Proxys vorhanden, wird die gesamte Systembelastung vom Hostsystem zu den Proxys verschoben. Sind keine Proxys vorhanden, bleibt die gesamte Belastung auf dem Host. Drosselung stellt sicher, dass mehrere VADP-Proxys optimal genutzt werden, um den Datendurchsatz zu maximieren. Bei jeder virtuellen Maschine, die gesichert werden soll, stellt IBM Spectrum Protect Plus fest, welcher VADP-Proxy am wenigsten ausgelastet ist und über den größten verfügbaren Speicher und die meisten freien Tasks verfügt.

Ist ein Proxy-Server vor dem Start des Jobs inaktiv oder anderweitig nicht verfügbar, übernehmen die anderen Proxys, um den Job auszuführen. Sind keine anderen Proxys vorhanden, übernimmt der Host den Job. Fällt ein Proxy-Server während der Ausführung eines Jobs aus, könnte der Job fehlschlagen.

Transportmodi beschreiben die Methode, mit der ein VADP-Proxy Daten versetzt. Der Transportmodus wird als Eigenschaft des Proxys definiert. In der Konfiguration der meisten Sicherungs- und Wiederherstellungsjobs wird später die Verwendung mindestens eines Proxys angegeben.

VADP-Proxys in IBM Spectrum Protect Plus unterstützen die folgenden VMware-Transportmodi: SAN, HotAdd, NBDSSL und NBD.

Auch wenn jedes Unternehmen anders ist und die Prioritäten bezüglich Größe, Geschwindigkeit, Zuverlässigkeit und Komplexität in jeder Umgebung unterschiedlich sind, gelten für die Auswahl des Transportmodus die folgenden allgemeinen Richtlinien:

- Der Transportmodus SAN sollte in einer direkten Speicherumgebung verwendet werden, weil dieser Modus schnell und im Allgemeinen zuverlässig ist.
- Der Transportmodus HotAdd sollte verwendet werden, wenn der VADP-Proxy virtualisiert ist. Dieser Modus unterstützt alle vSphere-Speichertypen.
- Der Transportmodus NBD oder NBDSSL (LAN) ist der Rückfallmodus, weil er in physischen, virtuellen und heterogenen Umgebungen funktioniert. In diesem Modus könnte jedoch die Datenübertragungsgeschwindigkeit beeinträchtigt sein, wenn die Netzverbindungen langsam sind. Der Modus NBDSSL unterscheidet sich vom Modus NBD nur dadurch, dass die zwischen dem VADP-Proxy und dem ESXi-Server übertragenen Daten bei Verwendung von NBDSSL verschlüsselt werden.

VADP-Proxys erstellen

Sie können VADP-Proxys für die Ausführung von VMware-Sicherungsjobs mit IBM Spectrum Protect Plus in Linux-Umgebungen erstellen.

Vorbereitende Schritte

Beachten Sie die folgenden Hinweise, bevor Sie VADP-Proxys erstellen:

- Überprüfen Sie die IBM Spectrum Protect Plus-Systemanforderungen in „VADP-Proxy-Anforderungen” auf Seite 17.
- Die IBM Spectrum Protect Plus-Version des VADP-Proxy-Installationsprogramms umfasst Virtual Disk Development Kit (VDDK) Version 6.5. Diese Version des VADP-Proxy-Installationsprogramms stellt externe VADP-Proxy-Unterstützung mit vSphere 6.5 bereit.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um VMware-VADP-Proxys zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **VADP-Proxy**.
2. Klicken Sie auf **Proxy registrieren**.
3. Füllen Sie die folgenden Felder im Fenster **VADP-Proxy installieren** aus:

   Hostname/IP

   Geben Sie die auflösbare IP-Adresse oder einen auflösbaren Pfad und Maschinennamen ein.

   Site auswählen

   Wählen Sie eine Site aus, die dem Proxy zugeordnet werden soll.

   Vorhandenen Benutzer verwenden

   Aktivieren Sie dieses Feld, um einen zuvor eingegebenen Benutzernamen und ein zuvor eingegebenes Kennwort für den Provider auszuwählen.

   Benutzername

   Geben Sie den Benutzernamen für den VADP-Proxy-Server ein.

   Kennwort

   Geben Sie das Kennwort für den VADP-Proxy-Server ein.
4. Klicken Sie auf **Installieren**.

   Der Proxy wird der Tabelle **VADP-Proxy** hinzugefügt.
5. Klicken Sie auf **Registrieren**, um den Proxy-Server zu registrieren.

   Mithilfe des Menüs **Aktionen** können Sie die Registrierung für den Server zurücknehmen oder den Server aussetzen. Durch das Aussetzen eines Proxys wird verhindert, dass bevorstehende Sicherungsjobs den Proxy verwenden. Jobs, die einen ausgesetzten Proxy oder einen Proxy, für den die Registrierung

zurückgenommen wurde, verwenden, werden lokal ausgeführt; dies kann sich auf die Leistung auswirken. Sie können Verwaltungstasks für den Proxy ausführen, während er ausgesetzt ist. Um die Verwendung des Proxys wiederaufzunehmen, wählen Sie **Aktionen** > **Wiederaufnehmen** aus.

Nach der erfolgreichen Registrierung wird der Service "vadp" auf der Proxy-Maschine gestartet. Eine Protokolldatei mit dem Namen `vadp.log` wird im Verzeichnis `/opt/IBM/SPP/logs` generiert.

6. Wiederholen Sie die vorherigen Schritte für jeden Proxy, der erstellt werden soll.

Die Verbindung zwischen der virtuellen IBM Spectrum Protect Plus-Appliance und einem registrierten VADP-Proxy ist eine bidirektionale Verbindung, die erfordert, dass die virtuelle IBM Spectrum Protect Plus-Appliance über Konnektivität zum VADP-Proxy und der VADP-Proxy über Konnektivität zur virtuellen IBM Spectrum Protect Plus-Appliance verfügt. Um sicherzustellen, dass einee korrekt Verbindung von der virtuellen IBM Spectrum Protect Plus-Appliance zum VADP-Proxy vorhanden ist, müssen Sie verifizieren, dass die virtuelle IBM Spectrum Protect Plus-Appliance den VADP-Proxy mit Ping überprüfen kann, indem Sie die folgenden Schritte ausführen:

1. Stellen Sie mithilfe des Netzprotokolls Secure Shell (SHH) die Verbindung zur Befehlszeile für die virtuelle IBM Spectrum Protect Plus-Appliance her.
2. Führen Sie `ping <VADP-IP>` aus; dabei ist <VADP-IP> die auflösbare IP-Adresse des VADP-Proxys.

Wenn der Pingbefehl fehlschlägt, stellen Sie sicher, dass die IP-Adresse des VADP-Proxys auflösbar und von der IBM Spectrum Protect Plus-Appliance erreichbar ist und dass eine Route von der IBM Spectrum Protect Plus-Appliance zum VADP-Proxy vorhanden ist. Wenn der Pingbefehl erfolgreich ist, stellen Sie sicher, dass eine korrekte Verbindung vom VADP-Proxy zur virtuellen IBM Spectrum Protect Plus-Appliance vorhanden ist, indem Sie die folgende Prozedur ausführen:

1. Stellen Sie mithilfe des Netzprotokolls Secure Shell (SHH) die Verbindung zur Befehlszeile für den VADP-Proxy her.
2. Führen Sie `ping <Spectrum_Protect_Plus-IP>` aus; dabei ist <Spectrum_Protect_Plus-IP> die auflösbare IP-Adresse der virtuellen IBM Spectrum Protect Plus-Appliance.

Wenn der Pingbefehl fehlschlägt, stellen Sie sicher, dass die IP-Adresse der virtuellen IBM Spectrum Protect Plus-Appliance auflösbar und vom VADP-Proxy erreichbar ist. Stellen Sie sicher, dass eine Route vom VADP-Proxy zur virtuellen IBM Spectrum Protect Plus-Appliance vorhanden ist.

Nächste Schritte

Führen Sie nach dem Erstellen der VADP-Proxys die folgende Aktion aus:

Aktion	Vorgehensweise
Führen Sie den VMware-Sicherungsjob aus.	Siehe „VMware-Daten sichern” auf Seite 107. Die Proxys werden im Jobprotokoll durch eine ähnliche Protokollnachricht wie die folgende angegeben: `Run remote vmdkbackup of MicroService: http://<Proxy>` *`Knotenname`*`, IP:`*`IP-Adresse_des_Proxys`*

Zugehörige Tasks

„Optionen für VADP-Proxys definieren” auf Seite 114
Sie können VADP-Proxys für die Ausführung von VMware-Sicherungsjobs mit IBM Spectrum Protect Plus in Linux-Umgebungen erstellen.

Optionen für VADP-Proxys definieren

Sie können VADP-Proxys für die Ausführung von VMware-Sicherungsjobs mit IBM Spectrum Protect Plus in Linux-Umgebungen erstellen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Optionen für VMware-VADP-Proxys zu definieren:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **VADP-Proxy**.
2. Klicken Sie auf das Symbol für Optionen ⋯, um die verfügbaren Optionen für den Proxy anzuzeigen.
3. Füllen Sie die folgenden Felder im Fenster **VADP-Proxy-Optionen definieren** aus:

   Site

   Ordnen Sie dem Proxy eine Site zu.

   Benutzer

   Wählen Sie einen zuvor eingegebenen Benutzernamen für den Provider aus. Um automatische Aktualisierungen des VADP-Proxys zu ermöglichen, muss ein zuvor eingegebener Benutzername ausgewählt werden.

   Transportmodi

   Legen Sie die Transportmodi fest, die vom Proxy verwendet werden sollen. Weitere Informationen zu VMware-Transportmodi finden Sie in Virtual Disk Transport Methods.

   NBDSSL-Komprimierung aktivieren

   Wenn Sie den Transportmodus NBDSSL ausgewählt hatten, aktivieren Sie die Komprimierung, um die Leistung bei Datenübertragungen zu verbessern.

   Um die Komprimierung zu inaktivieren, wählen Sie **Inaktiviert** aus.

   Protokollaufbewahrung in Tagen

   Legen Sie die Anzahl Tage für die Aufbewahrung von Protokollen fest, bevor die Protokolle gelöscht werden.

   Größe des Lese- und Schreibpuffers

   Legen Sie die Puffergröße der Datenübertragung (in Byte) fest.

   Blockgröße des NFS-Datenträgers

   Legen Sie die Blockgröße (in Byte) fest, die von dem bereitgestellten NFS-Datenträger verwendet werden soll.

   Softcap-Taskgrenzwert

   Legen Sie die Anzahl VMs fest, die ein Proxy gleichzeitig verarbeiten kann. Wenn **Alle Ressourcen verwenden** ausgewählt ist, wird der Taskgrenzwert auf der Basis der folgenden Formel durch die Anzahl CPUs im Proxy bestimmt:

   1 CPU = 1 VMDK

   Eine CPU ist die kleinste Hardwareeinheit, die einen Thread ausführen kann. Die Anzahl CPUs in einem Proxy wird mithilfe des Befehls `lscpu` bestimmt.

Nächste Schritte

Führen Sie nach der Erstellung der VADP-Proxys die folgenden Aktionen aus:

Aktion	Vorgehensweise
Führen Sie den VMware-Sicherungsjob aus.	Siehe „VMware-Daten sichern” auf Seite 107. Die Proxys werden im Jobprotokoll durch eine ähnliche Protokollnachricht wie die folgende angegeben: `Run remote vmdkbackup of MicroService: http://<Proxy` *`Knotenname`*`, IP:`*`IP-Adresse_des_Proxys`*
Deinstallieren Sie die Proxys, wenn keine VMware-Sicherungsjobs mehr ausgeführt werden.	Um einen Proxy zu deinstallieren, führen Sie den folgenden Befehl auf dem Hostsystem im Deinstallationsunterverzeichnis des Installationsverzeichnisses `/opt/IBM/SPP` aus: `./uninstall_vmdkbackup`

Zugehörige Tasks

„VADP-Proxys erstellen” auf Seite 113
Sie können VADP-Proxys für die Ausführung von VMware-Sicherungsjobs mit IBM Spectrum Protect Plus in Linux-Umgebungen erstellen.

VADP-Proxys deinstallieren

Sie können einen VADP-Proxy aus Ihrer IBM Spectrum Protect Plus-Umgebung entfernen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um VADP-Proxys in IBM Spectrum Protect Plus zu deinstallieren:

1. Navigieren Sie über eine Eingabeaufforderung zu dem Verzeichnis `/opt/IBM/SPP/uninstall` auf dem Proxy-Host-System.
2. Führen Sie den folgenden Befehl aus:
   `./uninstall_vmdkbackup`

VMware-Daten zurückschreiben

VMware-Zurückschreibungsjobs unterstützen Instant VM Restore- und Instant Disk Restore-Szenarios, die automatisch auf der Basis der ausgewählten Quelle erstellt werden.

Vorbereitende Schritte

Führen Sie die folgenden Tasks aus:

- Stellen Sie sicher, dass mindestens ein Mal ein VMware-Sicherungsjob ausgeführt wurde. Anweisungen finden Sie in „VMware-Daten sichern” auf Seite 107.
- Bevor ein IBM Spectrum Protect Plus-Benutzer Sicherungs- und Zurückschreibungsoperationen ausführen kann, müssen dem Benutzer Rollen zugeordnet werden. Erteilen Sie Benutzern mithilfe des Fensters **Accounts** Zugriff auf Hypervisoren und Sicherungs- und Zurückschreibungsoperationen. Rollen und zugehörige Berechtigungen werden während der Benutzeraccounterstellung zugeordnet. Weitere Informationen finden Sie in Kapitel 13, „Benutzerzugriff verwalten”, auf Seite 311 und „Benutzeraccounts verwalten” auf Seite 320.
- Die Größe einer virtuellen Maschine, die aus einer vSnap-Auslagerung in einen IBM Spectrum Protect-Zurückschreibungspunkt zurückgeschrieben wird, entspricht der mit Thick Provisioning definierten Größe der virtuellen Maschine, unabhängig von der Quellenbereitstellung aufgrund der Verwendung von NFS-Datenspeichern während der Auslagerung. Die vollständige Größe der Daten muss übertragen werden, auch wenn sie in der virtuellen Quellenmaschine nicht zugeordnet ist.

- Stellen Sie sicher, dass das Ziel, das für den Zurückschreibungsjob verwendet werden soll, in IBM Spectrum Protect Plus registriert ist. Diese Anforderung gilt für Zurückschreibungsjob, die Daten auf ursprüngliche Hosts oder Cluster zurückschreiben.
- Die Windows-Dateiindexierung und -Dateizurückschreibung auf Datenträger, die sich auf dynamischen Platten befinden, wird nicht unterstützt.
- Bei einer Zurückschreibung aus einem IBM Spectrum Protect-Archiv werden Dateien vom Band in einen Staging-Pool migriert, bevor der Job gestartet wird. Abhängig von der Größe der Zurückschreibung kann dieser Prozess mehrere Stunden dauern.

Informationen zu diesem Vorgang

Wird eine VMDK für die Zurückschreibungsoperation ausgewählt, zeigt IBM Spectrum Protect Plus automatisch Optionen für einen Instant Disk Restore-Job an, der Sofortschreibzugriff auf Daten und Anwendungszurückschreibungspunkte bereitstellt. Eine IBM Spectrum Protect Plus-Momentaufnahme wird einem Zielserver zugeordnet, auf dem bei Bedarf auf die Momentaufnahme zugegriffen und die Momentaufnahme wie erforderlich kopiert werden kann.

Alle anderen Quellen werden mit Instant VM Restore-Jobs zurückgeschrieben, die in den folgenden Modi ausgeführt werden können:

Testmodus
Im Testmodus werden temporäre virtuelle Maschinen für die Entwicklung oder den Test, die Momentaufnahmeverifizierung und die Verifizierung bei der Wiederherstellung nach einem Katastrophenfall auf einer geplanten, wiederholt anwendbaren Basis ohne Auswirkungen auf Produktionsumgebungen erstellt. Testmaschinen bleiben so lange aktiv, wie dies zur Ausführung des Tests und der Verifizierung erforderlich ist; anschließend werden sie gelöscht. Mithilfe des abgeschirmten Netzbetriebs können Sie eine sichere Umgebung erstellen, um Ihre Jobs zu testen, ohne dass Konflikte mit virtuellen Maschinen auftreten, die für die Produktion verwendet werden. Den virtuellen Maschinen, die im Testmodus erstellt werden, werden auch eindeutige Namen und IDs zugeordnet, um Konflikte innerhalb Ihrer Produktionsumgebung zu vermeiden. Anweisungen zum Erstellen eines abgeschirmten Netzes finden Sie in „Abgeschirmtes Netz durch einen VMware-Zurückschreibungsjob erstellen” auf Seite 123.

Klonmodus
Im Klonmodus werden Kopien von virtuellen Maschinen für Anwendungsfälle erstellt, die permanente Kopien oder Kopien mit langer Laufzeit für die Datenfilterung oder die Duplizierung einer Testumgebung in einem abgeschirmten Netz erfordern. Den virtuellen Maschinen, die im Klonmodus erstellt werden, werden auch eindeutige Namen und IDs zugeordnet, um Konflikte innerhalb Ihrer Produktionsumgebung zu vermeiden. Im Klonmodus müssen Sie auf die Ressourcenauslastung achten, da im Klonmodus permanente virtuelle Maschinen oder virtuelle Maschinen mit langer Laufzeit erstellt werden.

Produktionsmodus
Der Produktionsmodus ermöglicht die Wiederherstellung nach einem Katastrophenfall an der lokalen Site mithilfe von primärem Speicher oder an einer fernen Site für die Wiederherstellung nach einem Katastrophenfall, wobei ursprüngliche Systemimages durch Wiederherstellungsimages ersetzt werden. Alle Konfigurationen werden als Teil der Wiederherstellung übernommen, einschließlich Namen und IDs, und alle Jobs zum Kopieren von Daten, die der virtuellen Maschine zugeordnet sind, werden weiterhin ausgeführt.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen VMware-Zurückschreibungsjob zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **VMware** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch öffnen, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **VMware** klicken.

- Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Informationssymbol im Navigationsfenster des Assistenten.
- Um die optionalen Seiten im Assistenten zu übergehen, wählen Sie **Optionale Schritte überspringen** aus.

2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Aktionen aus:
   a) Überprüfen Sie die verfügbaren Quellen, einschließlich virtueller Maschinen (VMs) und virtueller Platten (VDisks). Wechseln Sie mithilfe des Filters **Sicht** zwischen den angezeigten Quellen, um Hosts und Cluster, VMs oder Tags und Kategorien anzuzeigen. Sie können eine Quelle erweitern, indem Sie auf ihren Namen klicken.

      Sie können auch den gesamten Namen oder einen Teil des Namens in das Kästchen **Suchen nach** eingeben, um VMs zu finden, die den Suchkriterien entsprechen. Sie können das Platzhalterzeichen (*) verwenden, um den gesamten oder einen Teil des Namens darzustellen. Beispielsweise steht vm2* für alle Ressourcen, deren Namen mit "vm2" beginnen.

   b) Klicken Sie auf das Plussymbol neben den Eintrag neben der Liste der Quellen, der der Zurückschreibungsliste hinzugefügt werden soll. Sie können mehrere Einträge desselben Typs (VM oder virtuelle Platte) hinzufügen.

      Um einen Eintrag aus der Zurückschreibungsliste zu entfernen, klicken Sie auf das Minussymbol neben dem Eintrag.

   c) Klicken Sie auf **Weiter**.
3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der VM oder virtuellen Platte an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren. Einige Felder werden erst angezeigt, nachdem ein zugehöriges Feld ausgewählt wurde.

Option	Beschreibung
Zurückschreibungstyp	Wählen Sie den Typ des Zurückschreibungsjobs aus: **Bedarfsgesteuert** Führt eine einmalige Zurückschreibungsoperation aus. **Wiederholt auftretend** Erstellt einen sich wiederholenden Job für die Zurückschreibung nach Zeitpunkt, der gemäß einem Zeitplan ausgeführt wird.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position aus, von der Daten zurückgeschrieben werden sollen: **Site** Die Site, an der Momentaufnahmen gesichert wurden. Die Site wird im Fenster **Systemkonfiguration** > **Site** definiert. **Cloudauslagerung** Der Cloud-Server, auf den Momentaufnahmen ausgelagert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Auslagerung** Der Repository-Server, auf den Momentaufnahmen ausgelagert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert. **Cloudarchivierung** Der Cloud-Server, auf dem Momentaufnahmen archiviert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert.

Option	Beschreibung
	Repository-Archivierung Der Repository-Server, auf dem Momentaufnahmen archiviert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus: **Demo** Die Demonstrationssite, von der Momentaufnahmen zurückgeschrieben werden sollen. **Primär** Die primäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. **Sekundär** Die sekundäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, wählen Sie einen Server im Menü **Position auswählen** aus.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Zurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Zurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datenbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wenn Sie Daten aus einer Cloudressource oder von einem Repository-Server zurückschreiben, wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben; wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert oder in einer Cloudressource oder auf einem Repository-Server archiviert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway auswählen.

4. Geben Sie auf der Seite **Ziel definieren** die Instanz an, die für jede ausgewählte Quelle verwendet werden soll, und klicken Sie auf **Weiter**:

   Ursprünglicher ESX-Host oder Cluster
   Wählen Sie diese Option aus, um Daten auf den ursprünglichen Host oder Cluster zurückzuschreiben.

   Alternativer ESX-Host oder Cluster
   Wählen Sie diese Option aus, um Daten in ein lokales Ziel zurückzuschreiben, das nicht mit dem ursprünglichen Host oder Cluster übereinstimmt; wählen Sie dann die alternative Position aus den verfügbaren Ressourcen aus. Test- und Produktionsnetze können an der alternativen Position konfiguriert werden, um ein abgeschirmtes Netz zu erstellen, das verhindert, dass zwischen den für den Test verwendeten virtuellen Maschinen und den für die Produktion verwendeten virtuellen Maschinen Konflikte auftreten. Wählen Sie im Abschnitt **vCenter** eine alternative Position aus. Die alternativen Positionen können nach Host oder Cluster gefiltert werden.

Geben Sie in das Feld **Ziel für VM-Ordner** den Ordnerpfad der virtuellen Maschine im Zieldatenspeicher ein. Beachten Sie, dass das Verzeichnis erstellt wird, wenn es nicht vorhanden ist. Verwenden Sie "/" als Stammorder der virtuellen Maschine des Zieldatenspeichers.

ESX-Host, wenn vCenter inaktiv ist
Wählen Sie diese Option aus, wenn das vCenter übergangen und Daten direkt auf den ESX-Host zurückgeschrieben werden sollen. In anderen Zurückschreibungsszenarios werden Aktionen vom vCenter ausgeführt. Wenn vCenter nicht verfügbar ist, werden mit dieser Option die virtuelle vCenter-Maschine oder die virtuellen vCenter-Maschinen zurückgeschrieben, von denen vCenter abhängig ist.

5. Führen Sie auf der Seite **Datenspeicher definieren** die folgenden Aktionen aus:
   - Wenn Sie Daten auf einen alternativen ESX-Host oder Cluster zurückschreiben, wählen Sie den Zieldatenspeicher aus und klicken Sie auf **Weiter**.
   - Wenn Sie Daten auf den ursprünglichen ESX-Host oder Cluster zurückschreiben, müssen Sie keinen Datenspeicher definieren. Klicken Sie auf **Weiter**.
6. Geben Sie auf der Seite **Netz definieren** die Netzeinstellungen an, die für jede ausgewählte Quelle verwendet werden sollen, und klicken Sie auf **Weiter**.
   - Wenn Sie Daten auf den ursprünglichen ESX-Host oder Cluster zurückschreiben, geben Sie die folgenden Netzeinstellungen an:

     System die Definition der IP-Konfiguration ermöglichen
     Wählen Sie diese Option aus, um Ihrem Betriebssystem die Definition der IP-Zieladresse zu ermöglichen. Während einer Zurückschreibungsoperation im Testmodus empfängt die virtuelle Zielmaschine eine neue MAC-Adresse zusammen mit einer zugeordneten NIC. Abhängig von Ihrem Betriebssystem kann eine neue IP-Adresse auf der Basis der ursprünglichen NIC der virtuellen Maschine oder durch DHCP zugeordnet werden. Während einer Zurückschreibung im Produktionsmodus wird die MAC-Adresse nicht geändert; daher sollte die IP-Adresse beibehalten werden.

     Ursprüngliche IP-Konfiguration verwenden
     Wählen Sie diese Option aus, um Daten mithilfe der vordefinierten IP-Adresskonfiguration auf den ursprünglichen Host oder Cluster zurückzuschreiben. Während der Zurückschreibungsoperation empfängt die virtuelle Zielmaschine eine neue MAC-Adresse, die IP-Adresse wird jedoch beibehalten.
   - Wenn Sie Daten auf einen alternativen ESX-Host oder Cluster zurückschreiben, führen Sie die folgenden Schritte aus:
     a. Legen Sie in den Feldern **Produktion** und **Test** virtuelle Netze für Ausführungen von Zurückschreibungsjobs im Produktions- und Testmodus fest. Zielnetzeinstellungen für Produktions- und Testumgebungen sollten auf verschiedene Positionen verweisen, um ein abgeschirmtes Netz zu erstellen, das verhindert, dass zwischen den für den Test verwendeten virtuellen Maschinen und den für die Produktion verwendeten virtuellen Maschinen Konflikte auftreten. Die Netze, die dem Test- und Produktionsmodus zugeordnet sind, werden verwendet, wenn der Zurückschreibungsjob im jeweiligen Modus ausgeführt wird.
     b. Definieren Sie eine IP-Adresse oder Teilnetzmaske für virtuelle Maschinen, die für Anwendungsfälle in der Entwicklung, im Test oder bei der Wiederherstellung nach einem Katastrophenfall wiederverwendet werden sollen. Unterstützte Zuordnungstypen umfassen IP zu IP, IP zu DHCP und Teilnetz zu Teilnetz. Virtuelle Maschinen mit mehreren NICs werden unterstützt.

        Führen Sie eine der folgenden Aktionen aus:
        - Um Ihrem Betriebssystem das Definieren der Zielteilnetze und IP-Adressen zu ermöglichen, klicken Sie auf **Systemdefinierte Teilnetze und IP-Adressen für VM-Gastbetriebssystem auf Ziel verwenden**.
        - Um Ihre vordefinierten Teilnetze und IP-Adressen zu verwenden, klicken Sie auf **Ursprüngliche Teilnetze und IP-Adressen für VM-Gastbetriebssystem auf Ziel verwenden**.
        - Um eine neue Zuordnungskonfiguration zu erstellen, wählen Sie **Zuordnungen für Teilnetze und IP-Adressen für VM-Gastbetriebssystem auf Ziel hinzufügen** aus, klicken Sie auf

Zuordnungen hinzufügen und geben Sie ein Teilnetz oder eine IP-Adresse in das Feld **Quellenteilnetz oder IP-Adresse hinzufügen** ein.

Wählen Sie eines der folgenden Netzprotokolle aus:

- Wählen Sie **DHCP** aus, um automatisch eine IP und zugehörige Konfigurationsdaten auszuwählen, wenn DHCP in der ausgewählten Quelle verfügbar ist.
- Wählen Sie **Statisch** aus, um ein bestimmtes Teilnetz oder eine bestimmte IP-Adresse, eine Teilnetzmaske, ein Gateway und ein DNS einzugeben. Die Felder **Teilnetz/IP-Adresse**, **Teilnetzmaske** und **Gateway** sind erforderliche Felder. Wird ein Teilnetz als Quelle eingegeben, muss auch ein Teilnetz als Ziel eingegeben werden.

Die IP-Rekonfiguration wird für virtuelle Maschinen übersprungen, wenn eine statische IP verwendet wird, aber keine geeignete Teilnetzzuordnung gefunden wird, oder wenn die virtuelle Quellenmaschine ausgeschaltet wird und mehrere zugeordnete NICs vorhanden sind. Wenn eine virtuelle Maschine in einer Windows-Umgebung nur DHCP verwendet, wird die IP-Rekonfiguration für diese virtuelle Maschine übersprungen. In einer Linux-Umgebung wird angenommen, dass alle Adressen statisch sind. Nur die IP-Zuordnung ist verfügbar.

7. Wählen Sie auf der Seite **Zurückschreibungsmethode** die Zurückschreibungsmethode aus, die für Quellenauswahlangaben verwendet werden soll. Definieren Sie, ob der VMware-Zurückschreibungsjob standardmäßig im Test-, Produktions- oder Klonmodus ausgeführt werden soll. Nachdem der Job erstellt wurde, kann er im Produktions- oder Klonmodus über das Fenster **Jobsitzungen** ausgeführt werden. Sie können den Namen der zurückgeschriebenen VM auch ändern, indem Sie den neuen Namen in das Feld **VM umbenennen (optional)** eingeben. Klicken Sie auf **Weiter**, um fortzufahren.
8. Konfigurieren Sie auf der Seite **Joboptionen (optional)** erweiterte Optionen und klicken Sie auf **Weiter**.

IA-Klonressource als permanent definieren
Aktivieren Sie diese Option, um die virtuelle Platte in den permanenten Speicher zu verschieben und temporäre Ressourcen zu löschen. Diese Aktion wird ausgeführt, indem eine vMotion-Operation für die Ressourcen im Hintergrund gestartet wird. Das Ziel der vMotion-Operation ist der VM-Konfigurationsdatenspeicher. Die Instant Access-Platte ist während dieser Operation weiterhin für Schreib-/Leseoperationen verfügbar.

Nach der Wiederherstellung einschalten
Wechseln Sie den Einschaltstatus einer virtuellen Maschine, nachdem eine Wiederherstellung ausgeführt wurde. Virtuelle Maschinen werden in der Reihenfolge eingeschaltet, in der sie wiederhergestellt werden (wie im Schritt für die Quelle definiert).

Einschränkung: Zurückgeschriebene VM-Schablonen können nach der Wiederherstellung nicht eingeschaltet werden.

Virtuelle Maschine überschreiben
Aktivieren Sie diese Option, um dem Zurückschreibungsjob das Überschreiben der ausgewählten virtuellen Maschine zu ermöglichen. Standardmäßig ist diese Option inaktiviert.

Mit Zurückschreibung fortfahren, auch wenn sie fehlschlägt
Aktivieren Sie diese Option, um mit der Wiederherstellung einer Ressource in einer Serie fortzufahren, wenn die Wiederherstellung der vorherigen Ressource fehlschlägt. Falls inaktiviert, wird der Zurückschreibungsjob gestoppt, wenn die Wiederherstellung einer Ressource fehlschlägt.

Bereinigung direkt beim Fehlschlagen des Jobs ausführen
Aktivieren Sie diese Option, um zugeordnete Ressourcen automatisch im Rahmen eines Zurückschreibungsjobs zu bereinigen, wenn die Wiederherstellung der virtuellen Maschine fehlschlägt.

Überschreiben zulassen und Bereinigung der anstehenden alten Sitzung erzwingen
Aktivieren Sie diese Option, wenn eine geplante Sitzung eines Wiederherstellungsjobs eine vorhandene anstehende Sitzung zwingen soll, zugeordnete Ressourcen zu bereinigen, sodass die neue Sitzung ausgeführt werden kann. Inaktivieren Sie diese Option, wenn eine vorhandene Testumgebung aktiv bleiben soll, ohne bereinigt zu werden.

VM-Tags zurückschreiben
Aktivieren Sie diese Option, um Tags zurückzuschreiben, die mit vSphere auf virtuelle Maschinen angewendet werden.

VMX-Datei wegen fehlender Platte korrigieren
Wenn einzelne Platten aus einer Sicherung ausgeschlossen werden, schlägt das Starten der zugeordneten virtuellen Maschine fehl. Aktivieren Sie diese Option, um die Einträge für ausgeschlossene Platten aus der VMX-Konfigurationsdatei zu entfernen, und stellen Sie sicher, dass die zurückgeschriebene virtuelle Maschine als Teil eines Instant VM Restore-Jobs gestartet wird.

An den Namen der virtuellen Maschine ein Suffix anhängen
Geben Sie ein Suffix ein, das an die Namen der zurückgeschriebenen virtuellen Maschinen angehängt werden soll.

Dem Namen der virtuellen Maschine ein Präfix voranstellen
Geben Sie ein Präfix ein, das den Namen der zurückgeschriebenen virtuellen Maschinen vorangestellt werden soll.

9. Optional: Wählen Sie auf der Seite **Scripts anwenden** die folgenden Scriptoptionen aus und klicken Sie auf **Weiter**.
   - Wählen Sie **Vorscript** aus, um ein hochgeladenes Script auszuwählen, und wählen Sie einen Anwendungs- oder Scriptserver aus, auf dem das Vorscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, auf dem das Script ausgeführt wird, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Rufen Sie die Seite **Systemkonfiguration** > **Script** auf, um Scripts und Scriptserver zu konfigurieren.
   - Wählen Sie **Nachscript** aus, um ein hochgeladenes Script auszuwählen, und wählen Sie einen Anwendungs- oder Scriptserver aus, auf dem das Nachscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, auf dem das Script ausgeführt wird, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Navigieren Sie zu der Seite **Systemkonfiguration** > **Script**, um Scripts und Scriptserver zu konfigurieren.
   - Wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus, um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt. Wenn diese Option aktiviert ist und das Vorscript mit einem Rückkehrcode ungleich null beendet wird, wird die Ausführung des Sicherungs- oder Zurückschreibungsjobs fortgesetzt und der Taskstatus für das Vorscript gibt ABGESCHLOSSEN zurück. Wenn ein Nachscript mit einem Rückkehrcode ungleich null beendet wird, gibt der Taskstatus für das Nachscript ABGESCHLOSSEN zurück. Wenn diese Option nicht ausgewählt wird, wird der Sicherungs- oder Zurückschreibungsjob nicht ausgeführt und der Taskstatus für das Vorscript oder Nachscript gibt FEHLGESCHLAGEN zurück.
10. Führen Sie auf der Seite **Zeitplan** eine der folgenden Aktionen aus:
    - Um einen bedarfsgesteuerten Job auszuführen, klicken Sie auf **Weiter**.
    - Um einen sich wiederholenden Job zu definieren, geben Sie einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an. Klicken Sie auf **Weiter**.
11. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs und klicken Sie auf **Übergeben**, um den Job zu erstellen.

    Bedarfsgesteuerte Jobs starten sofort; sich wiederholende Jobs starten zum geplanten Startzeitpunkt.

Nächste Schritte

Wählen Sie nach der Beendigung des Jobs eine der folgenden Optionen im Menü **Aktionen** im Abschnitt "Jobsitzungen" oder "Aktive Klone" im Fenster **Zurückschreibung** aus:

Bereinigen

Löscht die virtuelle Maschine und alle zugeordneten Ressourcen. Da dies eine temporäre virtuelle Maschine ist, die für den Test verwendet werden soll, gehen alle Daten verloren, wenn die virtuelle Maschine gelöscht wird.

In Produktion verschieben (vMotion)
Migriert die virtuelle Maschine über vMotion in den Datenspeicher und das als Produktionsnetz definierte virtuelle Netz.

Klonen (vMotion)
Migriert die virtuelle Maschine über vMotion in den Datenspeicher und das als Testnetz definierte virtuelle Netz.

Zugehörige Tasks

„vCenter Server-Instanz hinzufügen" auf Seite 99
Wenn IBM Spectrum Protect Plus eine vCenter Server-Instanz hinzugefügt wird, wird ein Bestand der Instanz erfasst, der es Ihnen ermöglicht, Sicherungs- und Zurückschreibungsjobs auszuführen und Berichte zu erstellen.

Abgeschirmtes Netz durch einen VMware-Zurückschreibungsjob erstellen

Mithilfe des abgeschirmten Netzbetriebs können Sie eine sichere Umgebung erstellen, um Ihre Jobs zu testen, ohne dass Konflikte mit virtuellen Maschinen auftreten, die für die Produktion verwendet werden. Der abgeschirmte Netzbetrieb kann mit Jobs verwendet werden, die im Testmodus und Produktionsmodus ausgeführt werden.

Vorbereitende Schritte

Erstellen Sie einen VMware-Zurückschreibungsjob und führen Sie ihn aus. Anweisungen finden Sie in „VMware-Daten zurückschreiben" auf Seite 116.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein abgeschirmtes Netz zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **VMware**.
2. Überprüfen Sie im Fenster **Zurückschreibung** die verfügbaren Zurückschreibungspunkte Ihrer VMware-Quellen, einschließlich der virtuellen Maschinen, VM-Schablonen, Datenspeicher, Ordner und vApps. Verwenden Sie die Suchfunktion und die Filter, um Ihre Auswahl für bestimmte Wiederherstellungssitetypen einzugrenzen. Erweitern Sie einen Eintrag im Fenster **Zurückschreibung**, um einzelne Zurückschreibungspunkte nach Datum anzuzeigen.
3. Wählen Sie Zurückschreibungspunkte aus und klicken Sie auf das Symbol für Hinzufügen zur Zurückschreibungsliste, um den Zurückschreibungspunkt zur Zurückschreibungsliste hinzuzufügen. Klicken Sie auf das Symbol für Entfernen, um Einträge aus der Zurückschreibungsliste zu entfernen.
4. Klicken Sie auf **Optionen**, um die Jobdefinitionsoptionen zu definieren.
5. Wählen Sie **Alternativer ESX-Host oder Cluster** aus und wählen Sie dann einen alternativen Host oder Cluster aus der vCenter-Liste aus.
6. Erweitern Sie den Abschnitt **Netzeinstellungen**. Definieren Sie mithilfe der Felder **Produktion** und **Test** virtuelle Netze für Ausführungen von Zurückschreibungsjobs im Produktions- und Testmodus. Zielnetzeinstellungen für Produktions- und Testumgebungen sollten verschiedene Positionen angeben, um ein abgeschirmtes Netz zu erstellen, das verhindert, dass zwischen den für den Test verwendeten virtuellen Maschinen und den für die Produktion verwendeten virtuellen Maschinen Konflikte auftreten. Die Netze, die dem Test und der Produktion zugeordnet werden, werden verwendet, wenn der Zurückschreibungsjob in dem jeweiligen Modus ausgeführt wird. Die IP-Adressen der Zielmaschine können mithilfe der folgenden Optionen konfiguriert werden:

   Systemdefinierte Teilnetze und IP-Adressen für VM-Gastbetriebssystem auf Ziel verwenden
   Wählen Sie diese Option aus, um Ihrem Betriebssystem die Definition der IP-Zieladresse zu ermöglichen. Während einer Zurückschreibung im Testmodus empfängt die virtuelle Zielmaschine eine neue MAC-Adresse zusammen mit einer zugeordneten NIC. Abhängig von Ihrem Betriebssystem kann eine neue IP-Adresse auf der Basis der ursprünglichen NIC der virtuellen Maschine oder durch DHCP zugeordnet werden. Während einer Zurückschreibungsoperation im Produktionsmodus wird die MAC-Adresse nicht geändert; daher sollte die IP-Adresse beibehalten werden.

Ursprüngliche Teilnetze und IP-Adressen für VM-Gastbetriebssystem auf Ziel verwenden
Wählen Sie diese Option aus, um Daten mithilfe der vordefinierten IP-Adresskonfiguration auf den ursprünglichen Host oder Cluster zurückzuschreiben. Während einer Zurückschreibung empfängt die virtuelle Zielmaschine eine neue MAC-Adresse, die IP-Adresse wird jedoch beibehalten.

Definieren Sie die Netzeinstellungen für eine Zurückschreibung auf einen alternativen oder fernen ESX-Host oder Cluster:

Definieren Sie mithilfe der Felder **Produktion** und **Test** virtuelle Netze für Ausführungen von Zurückschreibungsjobs im Produktions- und Testmodus. Zielnetzeinstellungen für Produktions- und Testumgebungen sollten verschiedene Positionen angeben, um ein abgeschirmtes Netz zu erstellen, das verhindert, dass zwischen den für den Test verwendeten virtuellen Maschinen und den für die Produktion verwendeten virtuellen Maschinen Konflikte auftreten. Die Netze, die dem Test und der Produktion zugeordnet werden, werden verwendet, wenn der Zurückschreibungsjob in dem jeweiligen Modus ausgeführt wird.

Definieren Sie eine IP-Adresse oder Teilnetzmaske für virtuelle Maschinen, die für Anwendungsfälle in der Entwicklung/im Test oder bei der Wiederherstellung nach einem Katastrophenfall wiederverwendet werden sollen. Unterstützte Zuordnungstypen umfassen IP zu IP, IP zu DHCP und Teilnetz zu Teilnetz. Virtuelle Maschinen mit mehreren NICs werden unterstützt.

Standardmäßig ist die Option **Systemdefinierte Teilnetze und IP-Adressen für VM-Gastbetriebssystem auf Ziel verwenden** aktiviert. Um Ihre vordefinierten Teilnetze und IP-Adressen zu verwenden, wählen Sie **Ursprüngliche Teilnetze und IP-Adressen für VM-Gastbetriebssystem auf Ziel verwenden** aus.

Um eine neue Zuordnungskonfiguration zu erstellen, wählen Sie **Zuordnungen für Teilnetze und IP-Adressen für VM-Gastbetriebssystem auf Ziel hinzufügen** aus und klicken Sie dann auf **Zuordnungen hinzufügen**. Geben Sie ein Teilnetz oder eine IP-Adresse in das Feld **Quelle** ein. Wählen Sie im Zielfeld **DHCP** aus, um automatisch eine IP und zugehörige Konfigurationsdaten auszuwählen, wenn DHCP auf dem ausgewählten Client verfügbar ist. Wählen Sie **Statisch** aus, um ein bestimmtes Teilnetz oder eine bestimmte IP-Adresse, eine Teilnetzmaske, ein Gateway und ein DNS einzugeben. Beachten Sie, dass **Teilnetz/IP-Adresse**, **Teilnetzmaske** und **Gateway** erforderliche Felder sind. Wird ein Teilnetz als Quelle eingegeben, muss auch ein Teilnetz als Ziel eingegeben werden.

Die IP-Rekonfiguration wird für virtuelle Maschinen übersprungen, wenn eine statische IP verwendet wird, aber keine geeignete Teilnetzzuordnung gefunden wird, oder wenn die Quellenmaschine ausgeschaltet wird und mehrere zugeordnete NICs vorhanden sind. Wenn eine virtuelle Maschine in einer Windows-Umgebung nur DHCP verwendet, wird die IP-Rekonfiguration für diese virtuelle Maschine übersprungen. In einer Linux-Umgebung wird angenommen, dass alle Adressen statisch sind. Nur die IP-Zuordnung ist verfügbar.

Zieldatenspeicher
Definieren Sie den Zieldatenspeicher für eine Zurückschreibung auf einen alternativen ESX-Host oder Cluster.

Ziel für VM-Ordner
Geben Sie den Pfad des VM-Ordners im Zieldatenspeicher ein. Beachten Sie, dass das Verzeichnis erstellt wird, wenn es nicht vorhanden ist. Verwenden Sie "/" als VM-Stammordner des Zieldatenspeichers.

7. Klicken Sie auf **Speichern**, um die Richtlinienoptionen zu speichern.
8. Wählen Sie nach der Beendigung des Jobs eine der folgenden Optionen im Menü **Aktionen** im Abschnitt "Jobsitzungen" oder "Aktive Klone" im Fenster **Zurückschreibung** aus:

Bereinigen

Löscht die virtuelle Maschine und alle zugeordneten Ressourcen. Da dies eine temporäre virtuelle Maschine/eine virtuelle Testmaschine ist, gehen alle Daten verloren, wenn die virtuelle Maschine gelöscht wird.

In Produktion verschieben (vMotion)

Migriert die virtuelle Maschine über vMotion in den Datenspeicher und das als "Produktionsnetz" definierte virtuelle Netz.

Klonen (vMotion)

Migriert die virtuelle Maschine über vMotion in den Datenspeicher und das als "Testnetz" definierte virtuelle Netz.

Zugehörige Tasks

„vCenter Server-Instanz hinzufügen” auf Seite 99
Wenn IBM Spectrum Protect Plus eine vCenter Server-Instanz hinzugefügt wird, wird ein Bestand der Instanz erfasst, der es Ihnen ermöglicht, Sicherungs- und Zurückschreibungsjobs auszuführen und Berichte zu erstellen.

Daten zurückschreiben, wenn der Zugriff auf vCenter oder andere Management-VMs nicht möglich ist

IBM Spectrum Protect Plus stellt eine Option bereit, um Daten automatisch unter Verwendung von ESXi-Hosts zurückzuschreiben, wenn der Zugriff auf vCenter nicht möglich ist. Mit dieser Option werden die virtuelle vCenter-Maschine oder die virtuellen vCenter-Maschinen zurückgeschrieben, von denen vCenter abhängig ist.

Informationen zu diesem Vorgang

Diese Prozedur kann verwendet werden, wenn einer der folgenden Management-Services in Ihrer Umgebung teilweise oder vollständig verloren geht:

- vCenter
- Platform Services Controller (PSC)
- Software-Defined Data Center (SDDC)
- Active Directory (AD)
- Domain Name System-Server (DNS-Server)

Um Daten ohne vCenter wiederherzustellen, muss der ESXi-Host über einen Standardswitch oder einen bereits vorhandenen verteilten Switch (Distributed Switch) mit ephemerer Bindung verfügen. Wenn diese Anforderungen nicht erfüllt sind, müssen Sie einen neuen Standardswitch auf dem ESXi-Host erstellen. Wenn für den Standardswitch keine Uplinks verfügbar sind, muss der Standardswitch aus dem verteilten Switch entfernt werden.

In der Prozedur sind die zusätzlichen manuellen Schritte beschrieben, die erforderlich sind, um eine Zurückschreibungsoperation auszuführen, wenn die Operation in einer vCenter Server-Umgebung (VCS-Umgebung) ausgeführt wird.

Die Wiederherstellung einer Management-VM in einer VCS-Umgebung kann dazu führen, dass der Zugriff auf die VM nicht mehr möglich ist. Ursache für den Verlust des Zugriffs ist eine fehlerhafte Konfiguration des virtuellen Switchs. Führen Sie die folgenden Schritte auf der betroffenen VM aus, um eine Wiederherstellungsoperation zur Wiederherstellung von diesem Zustand auszuführen.

Vorgehensweise

1. Stellen Sie die Verbindung zum ESXi-Zielbenutzerschnittstellenhost her und erstellen Sie einen neuen virtuellen Standardswitch. An diesem Punkt sind keine Portgruppen oder Uplinks für den Switch verfügbar.
2. Stellen Sie mithilfe des SSH-Protokolls die Verbindung zum ESXi-Server her. Identifizieren Sie die physische Netzschnittstellenkarte (NIC) und die Portgruppe des vorhandenen verteilten virtuellen Switchs (DVS), der den Namen SDDC-Dswitch-Private hat, und wählen Sie diese aus. Das folgende Beispiel referenziert eine virtualisierte Netzschnittstellenkarte (VNIC) mit dem Namen `vmnic0`, die zu Port-ID 64 gehört. Sie können die DVS-Informationen auflisten, indem Sie den folgenden Befehl ausgeben:

```
#esxcli network vswitch dvs vmware list
```

3. Entfernen Sie auf der Basis der vorherige Informationen mithilfe des folgenden Befehls die NIC und die Port-ID (Portgruppe) aus dem DVS SDDC-Dswitch-Private. Verwenden Sie die Port-ID aus Schritt 2.

   ```
   #esxcfg-vswitch -Q physische_VNIC -V Portgruppe SDDC-Dswitch-Private
   ```

4. Fügen Sie die NIC und die Portgruppe dem Standardswitch hinzu, der in Schritt 1 erstellt wurde, indem Sie den folgenden Befehl in einer einzigen Zeile ausgeben:

   ```
   #esxcli network vswitch standard uplink add –-uplink-name=physische_VNIC --vswitch-name=vir
   tueller_Standardswitch
   ```

5. Fügen Sie in der ESXi-Schnittstelle eine Portgruppe hinzu und wählen Sie den virtuellen Standardswitch aus.

   Der virtuelle Switch muss über 1 Uplink und 1 Portgruppe verfügen.

6. Führen Sie in IBM Spectrum Protect Plus eine Zurückschreibungsoperation mit aktivierter Option **ESX-Host, wenn vCenter inaktiv ist** aus.
7. Klicken Sie auf **Optionen**, wenn Sie die Zurückschreibungsoperation in IBM Spectrum Protect Plus definieren, und wählen Sie den neuen Netzswitch, der in Schritt 1 erstellt wurde, unter **Netzbetrieb** aus.
8. Schalten Sie unter Verwendung der ESXi-Zielbenutzerschnittstelle die wiederhergestellte VM ein.
9. Nachdem die VMs erreichbar sind, melden Sie sich bei der vCenter-Benutzerschnittstelle an und starten Sie die Migration der Management-VMs aus der temporären Portgruppe, die in Schritt 5 erstellt wurde, in die ursprüngliche verteilte Portgruppe SDDC-DPortGroup-Mgmt.

   Starten Sie auf der Registerkarte für den Netzbetrieb eine Migration, indem Sie ein Datencenter auswählen und dann im Aktionsmenü auf die Option zum Migrieren von VMs in ein anderes Netz klicken. Wählen Sie das Quellennetz (der in Schritt 5 erstellte temporäre Switch) und das Zielnetz (der Management-Switch) aus.

10. Nachdem alle VMs in die ursprüngliche Portgruppe migriert wurden, schließen Sie die physische NIC und die Portgruppe wieder in den ursprünglichen verteilten virtuellen Switch ein, indem Sie die folgenden Aktionen ausführen:

    a. Entfernen Sie die Netzkarten (die als VMNICs bezeichnet werden) aus einem virtuellen Standardswitch, der zuvor erneut zugeordnet wurde, indem Sie den folgenden Befehl ausgeben:

       ```
       #esxcli network vswitch standard uplink remove --uplink-name=VMNIC --vswitch-name=virtu
       eller_Switch
       ```

       Beispiel:

       ```
       #esxcli network vswitch standard uplink remove --uplink-name=vmnic0
       ```

       ```
       --vswitch-name=vered_recovery
       ```

    b. Fügen Sie einem vDS (vNetwork Distributed Switch) Netzkarten hinzu, indem Sie den folgenden Befehl ausgeben:

       ```
       #esxcfg-vswitch -P VMNIC -V nicht_verwendete_DV-Port-ID DVS # vDS-Uplink hinzufügen
       ```

       Beispiel:

       ```
       #esxcfg-vswitch -P vmnic0 -V 64 SDDC-Dswitch-Private
       ```

11. Löschen Sie die temporäre Portgruppe und den virtuellen Standardswitch aus der ESXi-Hostbenutzerschnittstelle.
12. Nachdem die VMs migriert wurden und auf sie zugegriffen werden kann, verwenden Sie die ESXi-Hostbenutzerschnittstelle, um die Registrierung der alten VMs zurückzunehmen (die VMs aber nicht zu löschen), wenn der ursprüngliche Host erreichbar ist. Mithilfe dieser Methode verhindern Sie die Erstellung doppelter Informationen, wie beispielsweise Namen, Media Access Control-(MAC-)Adres-

sen, Betriebssystemversions-IDs und Universal Unique Identifiers (UUIDs) für VMs. Sie müssen diesen Schritt selbst dann ausführen, wenn Sie einen neuen Datenspeicher verwenden.

In einigen vSphere- oder ESXi-Versionen kann die Operation zum Zurücknehmen der Registrierung mithilfe der Option zum Entfernen aus dem Bestand ausgeführt werden. Damit wird die Registrierung einer VM im vCenter-Katalog zurückgenommen, die VMDK-Dateien verbleiben jedoch im Datenspeicher und belegen dort Speicherbereich. Nachdem die VM vollständig wiederhergestellt wurde und die Umgebung erfolgreich ausgeführt wird, können Sie den Speicherbereich freigeben, indem Sie diese Dateien aus dem Datenspeicher entfernen.

Hyper-V-Daten sichern und zurückschreiben

Damit Hyper-V-Daten geschützt werden, müssen Sie zunächst Hyper-V-Server in IBM Spectrum Protect Plus hinzufügen und dann Jobs für Sicherungs- und Zurückschreibungsoperationen für den Inhalt der Server erstellen.

Stellen Sie sicher, dass Ihre Hyper-V-Umgebung die in „Hypervisoranforderungen” auf Seite 23 beschriebenen Systemanforderungen erfüllt.

Hyper-V-Server hinzufügen

Wenn IBM Spectrum Protect Plus ein Hyper-V-Server hinzugefügt wird, wird ein Bestand des Servers erfasst, der es Ihnen ermöglicht, Sicherungs- und Zurückschreibungsjobs auszuführen und Berichte zu erstellen.

Vorbereitende Schritte

Beachten Sie die folgenden Hinweise und Prozeduren, bevor Sie IBM Spectrum Protect Plus einen Hyper-V-Server hinzufügen:

- Hyper-V-Server können mithilfe eines DNS-Namens oder einer IP-Adresse registriert werden. DNS-Namen müssen von IBM Spectrum Protect Plus aufgelöst werden können. Wennn der Hyper-V-Server Teil eines Clusters ist, müssen alle Knoten in dem Cluster durch DNS aufgelöst werden können. Wenn DNS nicht verfügbar ist, muss der Server der Datei `/etc/hosts` auf der IBM Spectrum Protect Plus-Appliance hinzugefügt werden. Wenn mehrere Hyper-V-Server in einer Clusterumgebung definiert sind, müssen alle Server der Datei `/etc/hosts` hinzugefügt werden. Wenn der Cluster in IBM Spectrum Protect Plus registriert wird, registrieren Sie den Failovercluster-Manager.
- Für alle Hyper-V-Server, einschließlich Clusterknoten, muss der Microsoft-iSCSI-Initiator-Dienst in der Liste "Dienste" aktiv sein. Setzen Sie den Dienst auf "Automatisch", sodass er verfügbar ist, wenn die Maschine gebootet wird.
- Fügen Sie den Benutzer der lokalen Gruppe "Administratoren" auf dem Hyper-V-Server hinzu.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Hyper-V-Server hinzuzufügen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **Hyper-V**.
2. Klicken Sie auf **Hyper-V-Server verwalten**.
3. Klicken Sie auf **Hyper-V-Server hinzufügen**.
4. Füllen Sie die Felder im Fenster **Servereigenschaften** aus:

   Hostname/IP
   Geben Sie die auflösbare IP-Adresse oder einen auflösbaren Pfad und Maschinennamen ein.

   Vorhandenen Benutzer verwenden
   Aktivieren Sie dieses Feld, um einen zuvor eingegebenen Benutzernamen und ein zuvor eingegebenes Kennwort für den Server auszuwählen.

   Benutzername
   Geben Sie Ihren Benutzernamen für den Server ein.

Kennwort
Geben Sie Ihr Kennwort für den Server ein.

Port
Geben Sie den Kommunikationsport des Servers ein, der hinzugefügt wird. Der Standardport ist 5985.

Wählen Sie das Kontrollkästchen **SSL verwenden** aus, um eine verschlüsselte Secure Sockets Layer-Verbindung (SSL-Verbindung) zu aktivieren.

Um eine SSL-Verbindung zu aktivieren, müssen Sie das selbst signierte SSL-Zertifikat für den Hyper-V-Server oder ein Zertifikat von einer Zertifizierungsstelle (CA-Zertifikat) hinzufügen. Um ein Zertifikat hochzuladen, lesen Sie die Informationen in „SSL-Zertifikat über die Verwaltungskonsole hochladen" auf Seite 293.

Wird **SSL verwenden** nicht ausgewählt, müssen Sie zusätzliche Schritte auf dem Hyper-V-Server ausführen. Siehe „WinRM für Verbindung zu Hyper-V-Servern aktivieren" auf Seite 128.

5. Konfigurieren Sie im Abschnitt **Optionen** die folgende Option:

   Maximale Anzahl VMs, die pro Hyper-V-Server gleichzeitig verarbeitet werden sollen
   Definieren Sie die maximale Anzahl VM-Momentaufnahmen, die auf dem Hyper-V-Server gleichzeitig verarbeitet werden sollen.
6. Klicken Sie auf **Speichern**. IBM Spectrum Protect Plus bestätigt eine Netzverbindung, fügt den Server zur Datenbank hinzu und katalogisiert dann den Server.

   Wird eine Nachricht angezeigt, die angibt, dass die Verbindung nicht erfolgreich ist, überprüfen Sie Ihre Eingaben. Sind Ihre Eingaben korrekt und ist die Verbindung nicht erfolgreich, bitten Sie einen Systemadministrator, die Verbindungen zu überprüfen.

Nächste Schritte
Führen Sie die folgende Aktion aus, nachdem Sie den Hyper-V-Server hinzugefügt haben:

Aktion	Vorgehensweise
Fügen Sie dem Hypervisor Benutzerberechtigungen hinzu.	Siehe „Rolle erstellen" auf Seite 317.

Zugehörige Tasks
„Hyper-V-Daten sichern" auf Seite 129
Verwenden Sie einen Sicherungsjob, um Hyper-V-Daten mit Momentaufnahmen zu sichern.

„Hyper-V-Daten zurückschreiben" auf Seite 133
Hyper-V-Zurückschreibungsjobs unterstützen Instant VM Restore- und Instant Disk Restore-Szenarios, die auf der Basis der ausgewählten Quelle automatisch erstellt werden.

WinRM für Verbindung zu Hyper-V-Servern aktivieren
Wenn Sie SSL nicht verwenden können, um einen verschlüsselten Datenaustausch im Netz zwischen IBM Spectrum Protect Plus-Hyper-V-Servern zu aktivieren, müssen Sie WinRM auf dem Host konfigurieren, um einen nicht verschlüsselten Datenaustausch im Netz zu ermöglichen. Stellen Sie sicher, dass Sie die Sicherheitsrisiken verstehen, die mit einem nicht verschlüsselten Datenaustausch im Netz verbunden sind.

Vorgehensweise

Gehen Sie wie folgt vor, um WinRM für die Verbindung zu Hyper-V-Hosts zu konfigurieren:

1. Melden Sie sich auf dem Hyper-V-Hostsystem mit einem Administratoraccount an.
2. Öffnen Sie eine Windows-Eingabeaufforderung. Ist die Benutzeraccountsteuerung aktiviert, müssen Sie die Eingabeaufforderung mit erhöhten Rechten öffnen, indem die Option "Als Administrator ausführen" aktiviert wird.

3. Geben Sie den folgenden Befehl ein, um WinRM für nicht verschlüsselten Datenaustausch im Netz zu konfigurieren:

```
winrm s winrm/config/service @{AllowUnencrypted="true"}
```

4. Überprüfen Sie mit dem folgenden Befehl, ob die Option AllowUnencrypted auf 'true' gesetzt ist:

```
winrm g winrm/config/service
```

Hyper-V-Ressourcen erkennen
Hyper-V-Ressourcen werden automatisch erkannt, nachdem der Hyper-V-Server IBM Spectrum Protect Plus hinzugefügt wurde. Sie können jedoch einen Bestandsjob ausführen, um alle Änderungen zu finden, die seit dem Hinzufügen des Servers aufgetreten sind.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Bestandsjob auszuführen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **Hyper-V**.
2. Wählen Sie in der Liste der Hyper-V-Server einen Server aus oder klicken Sie auf den Link für den Server, um zu der gewünschten Ressource zu navigieren. Wenn beispielsweise ein Bestandsjob für eine einzelne virtuelle Maschine in einem Server ausgeführt werden soll, klicken Sie auf den Server-Link und wählen Sie dann eine virtuelle Maschine aus.
3. Klicken Sie auf **Bestandsverarbeitung ausführen**.

Verbindung zu einer virtuellen Maschine des Hyper-V-Servers testen
Sie können die Verbindung zu einer virtuellen Maschine des Hyper-V-Servers testen. Die Testfunktion verifiziert die Kommunikation mit der virtuellen Maschine und testet DNS-Einstellungen zwischen der virtuellen IBM Spectrum Protect-Appliance und der virtuellen Maschine.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Verbindung zu testen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **Hyper-V**.
2. Klicken Sie in der Liste der Hyper-V-Server auf den Link für eine virtuelle Maschine des Hyper-V-Servers, um zu den einzelnen virtuellen Maschinen zu navigieren.
3. Wählen Sie eine virtuelle Maschine aus und klicken Sie dann auf **Optionen auswählen**.
4. Wählen Sie **Vorhandenen Benutzer verwenden** aus.
5. Wählen Sie in der Liste **Benutzer auswählen** einen Benutzer aus.
6. Klicken Sie auf **Testen**.

Hyper-V-Daten sichern

Verwenden Sie einen Sicherungsjob, um Hyper-V-Daten mit Momentaufnahmen zu sichern.

Vorbereitende Schritte
Beachten Sie die folgenden Prozeduren und Hinweise, bevor Sie eine Sicherungsjobdefinition erstellen:

- Registrieren Sie die Provider, die gesichert werden sollen. Weitere Informationen finden Sie in „Hyper-V-Server hinzufügen” auf Seite 127.
- Konfigurieren Sie SLA-Richtlinien. Anweisungen finden Sie in „Sicherungsrichtlinien erstellen” auf Seite 75.
- Hyper-V-Sicherungs- und -Zurückschreibungsjobs erfordern die Installation der neuesten Hyper-V-Integrationsservices.

  Für Microsoft Windows-Umgebungen siehe Unterstützte Windows-Gastbetriebssysteme für Hyper-V unter Windows Server.

  Für Linux-Umgebungen siehe Unterstützte Linux- und FreeBSD-Computer für Hyper-V unter Windows.

- Für alle Hyper-V-Server, einschließlich Clusterknoten, muss der Microsoft-iSCSI-Initiator-Dienst in der Liste 'Dienste' aktiv sein. Setzen Sie den Dienst auf 'Automatisch', sodass er verfügbar ist, wenn die Maschine gebootet wird.
- Bevor ein IBM Spectrum Protect Plus-Benutzer Sicherungs- und Zurückschreibungsoperationen ausführen kann, müssen dem Benutzer Rollen zugeordnet werden. Erteilen Sie Benutzern mithilfe des Fensters **Accounts** Zugriff auf Hypervisoren und Sicherungs- und Zurückschreibungsoperationen. Rollen und zugehörige Berechtigungen werden während der Benutzeraccounterstellung zugeordnet. Weitere Informationen finden Sie in Kapitel 13, „Benutzerzugriff verwalten", auf Seite 311 und „Benutzeraccounts verwalten" auf Seite 320.
- Wenn eine virtuelle Maschine mehreren SLA-Richtlinien zugeordnet ist, stellen Sie sicher, dass die Richtlinien nicht gleichzeitig ausgeführt werden. Planen Sie die SLA-Richtlinien so, dass zwischen der Ausführung der einzelnen Richtlinien genügend Zeit ist, oder kombinieren Sie die Richtlinien in einer einzigen SLA-Richtlinie.
- Wird die IP-Adresse der IBM Spectrum Protect Plus-Appliance geändert, nachdem eine anfängliche Hyper-V-Basissicherung erstellt wurde, kann die Ziel-IQN der Hyper-V-Ressource einen ungültigen Status aufweisen. Um dieses Problem zu beheben, klicken Sie im Microsoft-iSCSI-Initiator-Tool auf die Registerkarte **Erkennung**. Wählen Sie die alte IP-Adresse aus und klicken Sie dann auf **Entfernen**. Klicken Sie auf die Registerkarte **Ziel** und trennen Sie die Verbindung zur Sitzung, für die die Verbindung wiederhergestellt wird.
- Wenn eine VM durch eine SLA-Richtlinie geschützt wird, werden die Sicherungen der VM abhängig von den Aufbewahrungsparametern der SLA-Richtlinie selbst dann beibehalten, wenn die VM entfernt wird.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Hyper-V-Sicherungsjob zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **Hyper-V**.
2. Wählen Sie Ressourcen aus, die gesichert werden sollen.

   Verwenden Sie die Suchfunktion, um nach verfügbaren Ressourcen zu suchen, und wechseln Sie mithilfe des Filters **Sicht** zwischen den angezeigten Ressourcen. Verfügbare Optionen sind **VMs** und **Datenspeicher**.
3. Klicken Sie auf **SLA-Richtlinie auswählen**, um eine oder mehrere SLA-Richtlinien, die Ihre Sicherungsdatenkriterien erfüllen, zur Jobdefinition hinzuzufügen.
4. Um die Jobdefinition mithilfe von Standardoptionen zu erstellen, klicken Sie auf **Speichern**.

   Der Job wird wie mit den von Ihnen ausgewählten SLA-Richtlinien definiert ausgeführt. Um den Job manuell auszuführen, klicken Sie auf **Jobs und Operationen** > **Zeitplan**. Wählen Sie den Job aus und klicken Sie auf **Aktionen** > **Starten**.

   Tipp: Die Schaltfläche **Ausführen** ist nur für die Sicherung eines einzelnen Hypervisors aktiviert; auf den Hypervisor muss außerdem eine SLA-Richtlinie angewendet sein.
5. Um Optionen vor dem Starten des Jobs zu editieren, klicken Sie in der Tabelle **Optionen auswählen** auf das Symbol für Editieren.

   Definieren Sie im Abschnitt **Sicherungsoptionen** die folgenden Jobdefinitionsoptionen:

   Schreibgeschützte Datenspeicher überspringen

   Aktivieren Sie diese Option, um Datenspeicher zu überspringen, die als schreibgeschützt bereitgestellt werden.

   Temporäre Datenspeicher überspringen, die für Instant Access bereitgestellt werden

   Aktivieren Sie diese Option, um temporäre Instant Access-Datenspeicher aus der Sicherungsjobdefinition auszuschließen.

   Priorität

   Definieren Sie die Sicherungspriorität der ausgewählten Ressource. Ressourcen mit einer höheren Priorität werden in dem Job zuerst gesichert. Klicken Sie im Abschnitt **VMware-Sicherung** auf die Ressource, der eine Priorität zugeordnet werden soll, und definieren Sie dann die Sicherungspriorität im

Feld **Priorität**. Definieren Sie 1 für die Ressource mit der höchsten Priorität oder 10 für die Ressource mit der geringsten Priorität. Wird kein Prioritätswert definiert, wird automatisch der Standardwert 5 zugeordnet.

Definieren Sie im Abschnitt **Momentaufnahmeoptionen** die folgenden Jobdefinitionsoptionen:

VM-Momentaufnahmeanwendung/Dateisystem konsistent machen

Aktivieren Sie diese Option, um die Anwendungs- oder Dateisystemkonsistenz für die VM-Momentaufnahme zu aktivieren.

Wiederholungsversuche für VM-Momentaufnahme

Definieren Sie, wie oft IBM Spectrum Protect Plus versuchen soll, eine Momentaufnahme einer virtuellen Maschine zu erstellen, bevor der Job abgebrochen wird.

Definieren Sie im Abschnitt **Agentenoptionen** die folgenden Jobdefinitionsoptionen:

SQL-Protokolle abschneiden

Um Anwendungsprotokolle für SQL während des Sicherungsjobs abzuschneiden, aktivieren Sie die Option **SQL-Protokolle abschneiden**. Beachten Sie, dass Berechtigungsnachweise für die zugeordnete virtuelle Maschine mithilfe der Optionen "Benutzername für Gastbetriebssystem" und "Kennwort für Gastbetriebssystem" in der Sicherungsjobdefinition erstellt werden müssen. Die Benutzeridentität folgt dem Standardformat *Domäne**Name*, wenn die virtuelle Maschine einer Domäne zugeordnet ist. Das Format *lokaler_Administrator* wird verwendet, wenn der Benutzer ein lokaler Administrator ist.

Die Benutzeridentität muss über Berechtigungen für den lokalen Administrator verfügen. Außerdem müssen auf dem SQL-Server für den Systemanmeldeberechtigungsnachweis SQL-Berechtigungen "sysadmin" sowie das Recht **Als Service anmelden** aktiviert werden. Weitere Informationen zu diesem Recht finden Sie in Add the Log on as a service Right to an Account.

IBM Spectrum Protect Plus generiert Protokolle, die die Protokollabschneidefunktion betreffen, und kopiert sie an die folgende Position auf der IBM Spectrum Protect Plus-Appliance:

```
/data/log/guestdeployer/spätestes_Datum/letzter_Eintrag/VM-Name
```

Dabei sind: *spätestes_Datum* ist das Datum, an dem der Sicherungsjob und die Protokollabschneidung ausgeführt wurden. *letzter_Eintrag* ist die UUID (Universal Unique Identifier) für den Job und *VM-Name* ist der Hostname oder die IP-Adresse der VM, auf der die Protokollabschneidung stattgefunden hat.

Einschränkung: Die Dateiindexierung und Dateizurückschreibung werden nicht von Zurückschreibungspunkten unterstützt, die auf einen IBM Spectrum Protect-Server ausgelagert wurden.

Dateimetadaten katalogisieren

Um die Dateiindexierung für die zugeordnete Momentaufnahme zu aktivieren, aktivieren Sie die Option "Dateimetadaten katalogisieren". Nach der Beendigung der Dateiindexierung können einzelne Dateien mithilfe des Fensters **Dateizurückschreibung** in IBM Spectrum Protect Plus zurückgeschrieben werden. Beachten Sie, dass Berechtigungsnachweise für die zugeordnete virtuelle Maschine mithilfe eines SSH-Schlüssels oder der Optionen "Benutzername für Gastbetriebssystem" und "Kennwort für Gastbetriebssystem" in der Sicherungsjobdefinition erstellt werden müssen. Stellen Sie sicher, dass von der IBM Spectrum Protect Plus-Appliance entweder mithilfe eines DNS oder Hostnamens auf die virtuelle Maschine zugegriffen werden kann. Beachten Sie, dass SSH-Schlüssel kein gültiger Berechtigungsmechanismus für Windows-Plattformen sind.

Dateien ausschließen

Geben Sie Verzeichnisse ein, die übersprungen werden sollen, wenn die Dateiindexierung ausgeführt wird. Dateien in diesen Verzeichnissen werden nicht dem IBM Spectrum Protect Plus-Katalog hinzugefügt und sind für die Dateiwiederherstellung nicht verfügbar. Verzeichnisse können mit einer exakten Übereinstimmung oder mit Sternen als Platzhalterzeichen, die vor dem Muster (*test) oder hinter dem Muster (test*) angegeben werden, ausgeschlossen werden. Mehrere Sterne als Platzhalterzeichen werden auch in einem einzelnen Muster unterstützt. Die Muster unterstützen alphanumerische Stan-

dardzeichen sowie die folgenden Sonderzeichen: - _ und *. Trennen Sie mehrere Filter durch ein Semikolon voneinander.

Vorhandenen Benutzer verwenden

Aktivieren Sie dieses Feld, um einen zuvor eingegebenen Benutzernamen und ein zuvor eingegebenes Kennwort für den Provider auszuwählen.

Benutzername/Kennwort für Gastbetriebssystem

Für einige Tasks (wie z. B. Katalogisierung von Dateimetadaten, Dateizurückschreibung und IP-Rekonfiguration) müssen für die zugeordnete virtuelle Maschine Berechtigungsnachweise erstellt werden. Geben Sie den Benutzernamen und das Kennwort ein und stellen Sie sicher, dass von der IBM Spectrum Protect Plus-Appliance entweder mithilfe eines DNS oder Hostnamens auf die virtuelle Maschine zugegriffen werden kann.

Die Standardsicherheitsrichtlinie verwendet das Windows-NTLM-Protokoll und die Benutzeridentität folgt dem Standardformat *Domäne\Name*, wenn die virtuelle Hyper-V-Maschine einer Domäne zugeordnet ist. Das Format *lokaler_Administrator* wird verwendet, wenn der Benutzer ein lokaler Administrator ist.

6. Um nach Fehlern bei einer Verbindung zu einer virtuellen Hypervisormaschine zu suchen, verwenden Sie die Funktion **Test**.

   Die Funktion **Test** verifiziert die Kommunikation mit der virtuellen Maschine und testet DNS-Einstellungen zwischen der IBM Spectrum Protect Plus-Appliance und der virtuellen Maschine. Um eine Verbindung zu testen, wählen Sie eine einzelne virtuelle Maschine aus und klicken Sie dann auf **Optionen auswählen**. Wählen Sie **Vorhandenen Benutzer verwenden** aus und wählen Sie einen zuvor eingegebenen Benutzernamen und ein zuvor eingegebenes Kennwort für die Ressource aus. Die Schaltfläche zum **Testen** wird rechts neben der Schaltfläche **Speichern** im Abschnitt **Optionen** angezeigt. Klicken Sie auf die Schaltfläche zum **Testen**.
7. Klicken Sie auf **Speichern**.
8. Um zusätzliche Optionen zu konfigurieren, klicken Sie auf das Feld **Richtlinienoptionen**, das dem Job im Abschnitt **SLA-Richtlinienstatus** zugeordnet ist. Definieren Sie die zusätzlichen Richtlinienoptionen:

   Vorscripts und Nachscripts

   Führen Sie ein Vorscript oder Nachscript aus. Vorscripts und Nachscripts sind Scripts, die vor oder nach der Ausführung eines Jobs auf Jobebene ausgeführt werden können. Windows-basierte Maschinen unterstützen Batch- und PowerShell-Scripts, während Linux-basierte Maschinen Shell-Scripts unterstützen.

   Wählen Sie im Abschnitt **Vorscript** oder **Nachscript** ein hochgeladenes Script und einen Scriptserver aus, auf dem das Script ausgeführt wird. Scripts und Scriptserver werden auf der Seite **Systemkonfiguration** > **Script** konfiguriert.

   Um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt, wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus.

   Wenn diese Option aktiviert wird und ein Vorscript oder Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird versucht, die Sicherungs- oder Zurückschreibungsoperation auszuführen, und der Taskstatus für das Vorscript wird als ABGESCHLOSSEN zurückgemeldet. Wenn ein Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird der Taskstatus für das Nachscript als ABGESCHLOSSEN zurückgemeldet.

   Wenn diese Option inaktiviert wird, wird nicht versucht, die Sicherung oder Zurückschreibung auszuführen, und der Taskstatus für das Vorscript oder Nachscript wird als FEHLGESCHLAGEN zurückgemeldet.

   Bestandsverarbeitung vor Sicherung ausführen

   Führen Sie einen Bestandsjob aus und erfassen Sie die neuesten Daten der ausgewählten Ressourcen, bevor Sie den Sicherungsjob starten.

   Ressourcen ausschließen

Schließen Sie bestimmte Ressourcen mit einzelnen oder mehreren Ausschlussmustern aus dem Sicherungsjob aus. Ressourcen können mit einer exakten Übereinstimmung oder mit Sternen als Platzhalterzeichen, die vor dem Muster (*test) oder hinter dem Muster (test*) angegeben werden, ausgeschlossen werden.

Mehrere Sterne als Platzhalterzeichen werden auch in einem einzelnen Muster unterstützt. Die Muster unterstützen alphanumerische Standardzeichen sowie die folgenden Sonderzeichen: - _ und *.

Trennen Sie mehrere Filter durch ein Semikolon voneinander.

Gesamtsicherung der Ressourcen erzwingen

Erzwingen Sie Basissicherungsoperationen für bestimmte virtuelle Maschinen oder Datenbanken in der Sicherungsjobdefinition. Trennen Sie mehrere Ressourcen durch ein Semikolon voneinander.

9. Um alle zusätzlichen Optionen zu speichern, die konfiguriert wurden, klicken Sie auf **Speichern**.

Nächste Schritte
Führen Sie die folgende Aktion aus, nachdem Sie einen Sicherungsjob definiert haben:

Aktion	Vorgehensweise
Erstellen Sie eine Hyper-V-Zurückschreibungsjobdefinition.	Siehe „Hyper-V-Daten zurückschreiben” auf Seite 133.

Zugehörige Konzepte
„Scripts für Sicherungs- und Zurückschreibungsoperationen konfigurieren” auf Seite 267
Vorscripts und Nachscripts sind Scripts, die ausgeführt werden können, bevor oder nachdem Sicherungs- und Zurückschreibungsjobs auf Jobebene ausgeführt werden. Unterstützt werden Shell-Scripts für Linux-basierte Systeme sowie Batch- und PowerShell-Scripts für Windows-basierte Systeme. Scripts werden lokal erstellt, über die Seite **Script** in Ihre Umgebung hochgeladen und dann auf Jobdefinitionen angewendet.

Zugehörige Tasks
„Jobs starten” auf Seite 264
Sie können einen Job selbst dann bedarfsgesteuert ausführen, wenn die Ausführung des Jobs gemäß einem Zeitplan festgelegt ist.

Hyper-V-Daten zurückschreiben

Hyper-V-Zurückschreibungsjobs unterstützen Instant VM Restore- und Instant Disk Restore-Szenarios, die auf der Basis der ausgewählten Quelle automatisch erstellt werden.

Vorbereitende Schritte
Führen Sie die folgenden Tasks aus:

- Stellen Sie sicher, dass mindestens ein Mal ein Hyper-V-Sicherungsjob ausgeführt wurde. Anweisungen finden Sie in „Hyper-V-Daten sichern” auf Seite 129.
- Stellen Sie sicher, dass das Ziel, das für den Zurückschreibungsjob verwendet werden soll, in IBM Spectrum Protect Plus registriert ist. Diese Anforderung gilt für Zurückschreibungsjob, die Daten auf ursprüngliche Hosts oder Cluster zurückschreiben.
- Stellen Sie sicher, dass die neuesten Hyper-V Integration Services installiert sind.

  Für Microsoft Windows-Umgebungen siehe Unterstützte Windows-Gastbetriebssysteme für Hyper-V unter Windows Server.

  Für Linux-Umgebungen siehe Unterstützte Linux- und FreeBSD-Computer für Hyper-V unter Windows.
- Stellen Sie sicher, dass die entsprechenden Rollen für Zurückschreibungsoperationen den betroffenen Benutzern zugeordnet sind. Erteilen Sie Benutzern im Fenster **Accounts** Zugriff auf Hypervisoren und Sicherungs- und Zurückschreibungsoperationen. Rollen und zugehörige Berechtigungen werden während der Benutzeraccounterstellung zugeordnet. Anweisungen finden Sie in Kapitel 13, „Benutzerzugriff verwalten”, auf Seite 311 und „Benutzeraccounts verwalten” auf Seite 320.

- Die Windows-Dateiindexierung und -Dateizurückschreibung auf Datenträger, die sich auf dynamischen Platten befinden, wird nicht unterstützt.
- Bei einer Zurückschreibung aus einem IBM Spectrum Protect-Archiv werden Dateien vom Band in einen Staging-Pool migriert, bevor der Job gestartet wird. Abhängig von der Größe der Zurückschreibung kann dieser Prozess mehrere Stunden dauern.

Informationen zu diesem Vorgang

Wird eine virtuelle Festplatte (VHDX = Virtual Hard Disk) für einen Zurückschreibungsjob ausgewählt, zeigt IBM Spectrum Protect Plus automatisch Optionen für einen Instant Disk Restore-Job an, der Sofortschreibzugriff auf Daten und Anwendungszurückschreibungspunkte bereitstellt.

Eine IBM Spectrum Protect Plus-Momentaufnahme wird einem Zielserver zugeordnet, auf dem bei Bedarf auf die Momentaufnahme zugegriffen und die Momentaufnahme wie erforderlich kopiert werden kann. Alle anderen Quellen werden mit Instant VM Restore-Jobs zurückgeschrieben, die in den folgenden Modi ausgeführt werden können:

Testmodus
Im Testmodus werden temporäre virtuelle Maschinen für die Entwicklung, den Test, die Momentaufnahmeverifizierung und die Verifizierung bei der Wiederherstellung nach einem Katastrophenfall auf einer geplanten, wiederholt anwendbaren Basis ohne Auswirkungen auf Produktionsumgebungen erstellt. Testmaschinen bleiben so lange aktiv, wie dies zur Ausführung des Tests und der Verifizierung erforderlich ist; anschließend werden sie gelöscht. Mithilfe des abgeschirmten Netzbetriebs können Sie eine sichere Umgebung erstellen, um Ihre Jobs zu testen, ohne dass Konflikte mit virtuellen Maschinen auftreten, die für die Produktion verwendet werden. Den virtuellen Maschinen, die im Testmodus erstellt werden, werden auch eindeutige Namen und IDs zugeordnet, um Konflikte innerhalb Ihrer Produktionsumgebung zu vermeiden.

Klonmodus
Im Klonmodus werden Kopien von virtuellen Maschinen für Anwendungsfälle erstellt, die permanente Kopien oder Kopien mit langer Laufzeit für die Datenfilterung oder die Duplizierung einer Testumgebung in einem abgeschirmten Netz erfordern. Den virtuellen Maschinen, die im Klonmodus erstellt werden, werden auch eindeutige Namen und IDs zugeordnet, um Konflikte innerhalb Ihrer Produktionsumgebung zu vermeiden. Im Klonmodus müssen Sie auf die Ressourcenauslastung achten, da im Klonmodus permanente virtuelle Maschinen oder virtuelle Maschinen mit langer Laufzeit erstellt werden.

Produktionsmodus
Der Produktionsmodus ermöglicht die Wiederherstellung nach einem Katastrophenfall an der lokalen Site mithilfe von primärem Speicher oder an einer fernen Site für die Wiederherstellung nach einem Katastrophenfall, wobei ursprüngliche Systemimages durch Wiederherstellungsimages ersetzt werden. Alle Konfigurationen werden als Teil der Wiederherstellung übernommen, einschließlich Namen und IDs, und alle Jobs zum Kopieren von Daten, die der virtuellen Maschine zugeordnet sind, werden weiterhin ausgeführt.

Einschränkung: Der Wechsel vom Testmodus zum Produktionsmodus wird für Hyper-V nicht unterstützt.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Hyper-V-Zurückschreibungsjob zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Hypervisoren** > **Hyper-V** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch öffnen, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **Hyper-V** klicken.
   - Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Informationssymbol im Navigationsfenster des Assistenten.

- Um die optionalen Seiten im Assistenten zu übergehen, wählen Sie **Optionale Schritte überspringen** aus.

2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Aktionen aus:
   a) Überprüfen Sie die verfügbaren Quellen, einschließlich virtueller Maschinen (VMs) und virtueller Platten (VDisks). Sie können eine Quelle erweitern, indem Sie auf ihren Namen klicken.

      Sie können auch den gesamten Namen oder einen Teil des Namens in das Kästchen **Suchen nach** eingeben, um VMs zu finden, die den Suchkriterien entsprechen. Sie können das Platzhalterzeichen (*) verwenden, um den gesamten oder einen Teil des Namens darzustellen. Beispielsweise steht `vm2*` für alle Ressourcen, deren Namen mit "vm2" beginnen.

   b) Klicken Sie auf das Plussymbol  neben den Eintrag neben der Liste der Quellen, der der Zurückschreibungsliste hinzugefügt werden soll. Sie können mehrere Einträge desselben Typs (VM oder virtuelle Platte) hinzufügen.

      Um einen Eintrag aus der Zurückschreibungsliste zu entfernen, klicken Sie auf das Minussymbol  neben dem Eintrag.

   c) Klicken Sie auf **Weiter**.

3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der VM oder virtuellen Platte an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren. Einige Felder werden erst angezeigt, nachdem ein zugehöriges Feld ausgewählt wurde.

Option	Beschreibung
Zurückschreibungstyp	Wählen Sie den Typ des Zurückschreibungsjobs aus: **Bedarfsgesteuert** Führt eine einmalige Zurückschreibungsoperation aus. **Wiederholt auftretend** Erstellt einen sich wiederholenden Job für die Zurückschreibung nach Zeitpunkt, der gemäß einem Zeitplan ausgeführt wird.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position aus, von der Daten zurückgeschrieben werden sollen: **Site** Die Site, an der Momentaufnahmen gesichert wurden. Die Site wird im Fenster **Systemkonfiguration** > **Site** definiert. **Cloudauslagerung** Der Cloud-Server, auf den Momentaufnahmen ausgelagert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Auslagerung** Der Repository-Server, auf den Momentaufnahmen ausgelagert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert. **Cloudarchivierung** Der Cloud-Server, auf dem Momentaufnahmen archiviert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Archivierung** Der Repository-Server, auf dem Momentaufnahmen archiviert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus:

Option	Beschreibung
	Demo Die Demonstrationssite, von der Momentaufnahmen zurückgeschrieben werden sollen. **Primär** Die primäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. **Sekundär** Die sekundäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, wählen Sie einen Server im Menü **Position auswählen** aus.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Zurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Zurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datenbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wenn Sie Daten aus einer Cloudressource oder von einem Repository-Server zurückschreiben, wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben; wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert oder in einer Cloudressource oder auf einem Repository-Server archiviert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway auswählen.

4. Wählen Sie auf der Seite **Ziel definieren** die Instanz aus, die für die ausgewählte Quelle zurückgeschrieben werden soll, und klicken Sie auf **Weiter**:

   Ursprünglicher Hyper-V-Host oder Cluster
   Wählen Sie diese Option aus, um Daten auf den ursprünglichen Host oder Cluster zurückzuschreiben.

   Alternativer Hyper-V-Host oder Cluster
   Wählen Sie diese Option aus, um Daten in ein lokales Ziel zurückzuschreiben, das nicht mit dem ursprünglichen Host oder Cluster übereinstimmt; wählen Sie dann die alternative Position aus den verfügbaren Ressourcen aus.

   Geben Sie in das Feld **Ziel für VM-Ordner** den Ordnerpfad der virtuellen Maschine im Zieldatenspeicher ein. Beachten Sie, dass das Verzeichnis erstellt wird, wenn es nicht vorhanden ist. Verwenden Sie "/" als Stammorder der virtuellen Maschine des Zieldatenspeichers.

5. Führen Sie auf der Seite **Datenspeicher definieren** die folgenden Aktionen aus:

   - Wenn Sie Daten auf einen alternativen Hyper-V-Host oder Cluster zurückschreiben, wählen Sie den Zieldatenspeicher aus und klicken Sie auf **Weiter**.
   - Wenn Sie Daten auf den ursprünglichen ESX-Host oder Cluster zurückschreiben, müssen Sie keinen Datenspeicher definieren. Klicken Sie einfach auf **Weiter**.

6. Geben Sie auf der Seite **Netz definieren** die Netzeinstellungen an, die für jede ausgewählte Quelle verwendet werden sollen, und klicken Sie auf **Weiter**.

- Wenn Sie Daten auf den ursprünglichen Hyper-V-Host oder Cluster zurückschreiben, geben Sie die folgenden Netzeinstellungen an:

  System die Definition der IP-Konfiguration ermöglichen
  Wählen Sie diese Option aus, um Ihrem Betriebssystem die Definition der IP-Zieladresse zu ermöglichen. Während einer Zurückschreibungsoperation im Testmodus empfängt die virtuelle Zielmaschine eine neue MAC-Adresse zusammen mit einer zugeordneten NIC. Abhängig von Ihrem Betriebssystem kann eine neue IP-Adresse auf der Basis der ursprünglichen NIC der virtuellen Maschine oder durch DHCP zugeordnet werden. Während einer Zurückschreibung im Produktionsmodus wird die MAC-Adresse nicht geändert; daher sollte die IP-Adresse beibehalten werden.

  Ursprüngliche IP-Konfiguration verwenden
  Wählen Sie diese Option aus, um Daten mithilfe der vordefinierten IP-Adresskonfiguration auf den ursprünglichen Host oder Cluster zurückzuschreiben. Während der Zurückschreibungsoperation empfängt die virtuelle Zielmaschine eine neue MAC-Adresse, die IP-Adresse wird jedoch beibehalten.

- Wenn Sie Daten auf einen alternativen Hyper-V-Host oder Cluster zurückschreiben, führen Sie die folgenden Schritte aus:

  a. Legen Sie in den Feldern **Produktion** und **Test** virtuelle Netze für Ausführungen von Zurückschreibungsjobs im Produktions- und Testmodus fest. Zielnetzeinstellungen für Produktions- und Testumgebungen sollten auf verschiedene Positionen verweisen, um ein abgeschirmtes Netz zu erstellen, das verhindert, dass zwischen den für den Test verwendeten virtuellen Maschinen und den für die Produktion verwendeten virtuellen Maschinen Konflikte auftreten. Die Netze, die dem Test- und Produktionsmodus zugeordnet sind, werden verwendet, wenn der Zurückschreibungsjob im jeweiligen Modus ausgeführt wird.

  b. Definieren Sie eine IP-Adresse oder Teilnetzmaske für virtuelle Maschinen, die für Anwendungsfälle in der Entwicklung, im Test oder bei der Wiederherstellung nach einem Katastrophenfall wiederverwendet werden sollen. Unterstützte Zuordnungstypen umfassen IP zu IP, IP zu DHCP und Teilnetz zu Teilnetz. Virtuelle Maschinen mit mehreren NICs werden unterstützt.

     Führen Sie eine der folgenden Aktionen aus:

     – Um Ihrem Betriebssystem das Definieren der Zielteilnetze und IP-Adressen zu ermöglichen, klicken Sie auf **Systemdefinierte Teilnetze und IP-Adressen für VM-Gastbetriebssystem auf Ziel verwenden**.
     – Um Ihre vordefinierten Teilnetze und IP-Adressen zu verwenden, klicken Sie auf **Ursprüngliche Teilnetze und IP-Adressen für VM-Gastbetriebssystem auf Ziel verwenden**.
     – Um eine neue Zuordnungskonfiguration zu erstellen, wählen Sie **Zuordnungen für Teilnetze und IP-Adressen für VM-Gastbetriebssystem auf Ziel hinzufügen** aus, klicken Sie auf **Zuordnungen hinzufügen** und geben Sie ein Teilnetz oder eine IP-Adresse in das Feld **Quellenteilnetz oder IP-Adresse hinzufügen** ein.

       Wählen Sie eines der folgenden Netzprotokolle aus:

       - Wählen Sie **DHCP** aus, um automatisch eine IP und zugehörige Konfigurationsdaten auszuwählen, wenn DHCP in der ausgewählten Quelle verfügbar ist.
       - Wählen Sie **Statisch** aus, um ein bestimmtes Teilnetz oder eine bestimmte IP-Adresse, eine Teilnetzmaske, ein Gateway und ein DNS einzugeben. Die Felder **Teilnetz/IP-Adresse**, **Teilnetzmaske** und **Gateway** sind erforderliche Felder. Wird ein Teilnetz als Quelle eingegeben, muss auch ein Teilnetz als Ziel eingegeben werden.

       Die IP-Rekonfiguration wird für virtuelle Maschinen übersprungen, wenn eine statische IP verwendet wird, aber keine geeignete Teilnetzzuordnung gefunden wird, oder wenn die virtuelle Quellenmaschine ausgeschaltet wird und mehrere zugeordnete NICs vorhanden sind. Wenn eine virtuelle Maschine in einer Windows-Umgebung nur DHCP verwendet, wird die IP-Rekonfiguration für diese virtuelle Maschine übersprungen. In einer Linux-Umgebung wird angenommen, dass alle Adressen statisch sind. Nur die IP-Zuordnung ist verfügbar.

7. Wählen Sie auf der Seite **Zurückschreibungsmethode** die Zurückschreibungsmethode aus, die für Quellenauswahlangaben verwendet werden soll. Definieren Sie, ob der Hyper-V-Zurückschreibungsjob standardmäßig im Test-, Produktions- oder Klonmodus ausgeführt werden soll. Nachdem der Job erstellt wurde, kann der Job mithilfe des Fensters **Jobsitzungen** im Produktions- oder Klonmodus ausgeführt werden. Sie können den Namen der zurückgeschriebenen VM auch ändern, indem Sie den neuen Namen in das Feld **VM umbenennen (optional)** eingeben. Klicken Sie auf **Weiter**, um fortzufahren.
8. Optional: Konfigurieren Sie auf der Seite **Joboptionen (optional)** erweiterte Optionen und klicken Sie auf **Weiter**.

   IA-Klonressource als permanent definieren
   Aktivieren Sie diese Option, um die virtuelle Platte in den permanenten Speicher zu verschieben und temporäre Ressourcen zu löschen. Diese Aktion wird ausgeführt, indem eine vMotion-Operation für die Ressourcen im Hintergrund gestartet wird. Das Ziel der vMotion-Operation ist der VM-Konfigurationsdatenspeicher. Die Instant Access-Platte ist während dieser Operation weiterhin für Schreib-/Leseoperationen verfügbar.

   Nach der Wiederherstellung einschalten
   Wechseln Sie den Einschaltstatus einer virtuellen Maschine, nachdem eine Wiederherstellung ausgeführt wurde. Virtuelle Maschinen werden in der Reihenfolge eingeschaltet, in der sie wiederhergestellt werden (wie im Schritt für die Quelle definiert).

   Einschränkung: Zurückgeschriebene VM-Schablonen können nach der Wiederherstellung nicht eingeschaltet werden.

   Virtuelle Maschine überschreiben
   Aktivieren Sie diese Option, um dem Zurückschreibungsjob das Überschreiben der ausgewählten virtuellen Maschine zu ermöglichen. Standardmäßig ist diese Option inaktiviert.

   Mit Zurückschreibung fortfahren, auch wenn sie fehlschlägt
   Aktivieren Sie diese Option, um mit der Wiederherstellung einer Ressource in einer Serie fortzufahren, wenn die Wiederherstellung der vorherigen Ressource fehlschlägt. Falls inaktiviert, wird der Zurückschreibungsjob gestoppt, wenn die Wiederherstellung einer Ressource fehlschlägt.

   Bereinigung direkt beim Fehlschlagen des Jobs ausführen
   Aktivieren Sie diese Option, um zugeordnete Ressourcen automatisch im Rahmen eines Zurückschreibungsjobs zu bereinigen, wenn die Wiederherstellung der virtuellen Maschine fehlschlägt.

   Überschreiben zulassen und Bereinigung der anstehenden alten Sitzung erzwingen
   Aktivieren Sie diese Option, wenn eine geplante Sitzung eines Wiederherstellungsjobs eine vorhandene anstehende Sitzung zwingen soll, zugeordnete Ressourcen zu bereinigen, sodass die neue Sitzung ausgeführt werden kann. Inaktivieren Sie diese Option, wenn eine vorhandene Testumgebung aktiv bleiben soll, ohne bereinigt zu werden.

   An den Namen der virtuellen Maschine ein Suffix anhängen
   Geben Sie ein Suffix ein, das an die Namen der zurückgeschriebenen virtuellen Maschinen angehängt werden soll.

   Dem Namen der virtuellen Maschine ein Präfix voranstellen
   Geben Sie ein Präfix ein, das den Namen der zurückgeschriebenen virtuellen Maschinen vorangestellt werden soll. Klicken Sie auf "Speichern", um die Richtlinienoptionen zu speichern.
9. Optional: Wählen Sie auf der Seite **Scripts anwenden** die folgenden Scriptoptionen aus und klicken Sie auf **Weiter**.

   - Wählen Sie **Vorscript** aus, um ein hochgeladenes Script auszuwählen, und wählen Sie einen Anwendungs- oder Scriptserver aus, auf dem das Vorscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, auf dem das Script ausgeführt wird, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Rufen Sie die Seite **Systemkonfiguration** > **Script** auf, um Scripts und Scriptserver zu konfigurieren.
   - Wählen Sie **Nachscript** aus, um ein hochgeladenes Script auszuwählen, und wählen Sie einen Anwendungs- oder Scriptserver aus, auf dem das Nachscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, auf dem das Script ausgeführt wird, wählen Sie das Kontrollkästchen

Scriptserver verwenden ab. Navigieren Sie zu der Seite **Systemkonfiguration** > **Script**, um Scripts und Scriptserver zu konfigurieren.

- Wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus, um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt. Wenn diese Option aktiviert ist und das Vorscript mit einem Rückkehrcode ungleich null beendet wird, wird die Ausführung des Sicherungs- oder Zurückschreibungsjobs fortgesetzt und der Taskstatus für das Vorscript gibt ABGESCHLOSSEN zurück. Wenn ein Nachscript mit einem Rückkehrcode ungleich null beendet wird, gibt der Taskstatus für das Nachscript ABGESCHLOSSEN zurück. Wenn diese Option nicht ausgewählt wird, wird der Sicherungs- oder Zurückschreibungsjob nicht ausgeführt und der Taskstatus für das Vorscript oder Nachscript gibt FEHLGESCHLAGEN zurück.

10. Führen Sie auf der Seite **Zeitplan** eine der folgenden Aktionen aus:
    - Um einen bedarfsgesteuerten Job auszuführen, klicken Sie auf **Weiter**.
    - Um einen sich wiederholenden Job zu definieren, geben Sie einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an. Klicken Sie auf **Weiter**.
11. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs und klicken Sie auf **Übergeben**, um den Job zu erstellen.

    Bedarfsgesteuerte Jobs starten sofort; sich wiederholende Jobs starten zum geplanten Startzeitpunkt.

Nächste Schritte

Wählen Sie nach der Beendigung des Jobs eine der folgenden Optionen im Menü **Aktionen** im Abschnitt **Jobsitzungen** oder **Aktive Klone** im Fenster **Zurückschreibung** aus:

Bereinigen
Löscht die virtuelle Maschine und alle zugeordneten Ressourcen. Da dies eine temporäre virtuelle Maschine ist, die für den Test verwendet werden soll, gehen alle Daten verloren, wenn die virtuelle Maschine gelöscht wird.

Klonen (migrieren)
Migriert die virtuelle Maschine in den Datenspeicher und das virtuelle Netz, die als Testnetz definiert sind.

Zugehörige Tasks

„Hyper-V-Daten sichern” auf Seite 129
Verwenden Sie einen Sicherungsjob, um Hyper-V-Daten mit Momentaufnahmen zu sichern.

„Hyper-V-Server hinzufügen” auf Seite 127
Wenn IBM Spectrum Protect Plus ein Hyper-V-Server hinzugefügt wird, wird ein Bestand des Servers erfasst, der es Ihnen ermöglicht, Sicherungs- und Zurückschreibungsjobs auszuführen und Berichte zu erstellen.

Dateien zurückschreiben

Stellen Sie Dateien aus Momentaufnahmen wieder her, die von IBM Spectrum Protect Plus-Sicherungsjobs erstellt werden. Dateien können an ihre ursprüngliche Position oder an eine alternative Position zurückgeschrieben werden.

Vorbereitende Schritte

Beachten Sie die folgenden Prozeduren und Hinweise, bevor Sie eine Datei zurückschreiben:

- Überprüfen Sie die Dateiindexierungs- und Zurückschreibungsanforderungen in „Dateiindexierungs- und -zurückschreibungsanforderungen” auf Seite 24.
- Führen Sie einen Sicherungsjob mit aktivierter Option "Dateimetadaten katalogisieren" aus. Beachten Sie die folgenden Richtlinien:

– Stellen Sie sicher, dass Berechtigungsnachweise sowohl für die zugeordnete virtuelle Maschine als auch für das alternative Ziel der virtuellen Maschine mithilfe der Optionen "Benutzername für Gastbetriebssystem" und "Kennwort für Gastbetriebssystem" in der Sicherungsjobdefinition erstellt werden.
– Stellen Sie sicher, dass von der IBM Spectrum Protect Plus-Appliance entweder über einen DNS oder einen Hostnamen auf die virtuelle Maschine zugegriffen werden kann. In einer Windows-Umgebung verwendet die Standardsicherheitsrichtlinie das Windows-NTLM-Protokoll und die Benutzeridentität folgt dem Standardformat *Domäne**Name*, wenn die virtuelle Hyper-V-Maschine einer Domäne zugeordnet ist. Das Format *lokaler_Administrator* wird verwendet, wenn der Benutzer ein lokaler Administrator ist.
– Damit eine Dateizurückschreibung erfolgreich ausgeführt werden kann, müssen Sie sicherstellen, dass die Benutzer-ID auf der Zielmaschine über die erforderlichen Eigentumsberechtigungen für die Datei verfügt, die zurückgeschrieben wird. Wenn eine Datei von einem Benutzer mit einer Benutzer-ID erstellt wurde, die nicht mit der des Benutzers übereinstimmt, der die Datei auf der Basis von Windows-Sicherheitsberechtigungsnachweisen zurückschreibt, schlägt der Dateizurückschreibungsjob fehl.

Informationen zu diesem Vorgang

Einschränkungen:

- Verschlüsselte Windows-Dateisysteme werden für die die Katalogisierung von Dateien oder für die Dateizurückschreibung nicht unterstützt.
- Die Dateiindexierung und Dateizurückschreibung werden nicht von Zurückschreibungspunkten unterstützt, die in Cloudressourcen oder auf Repository-Server ausgelagert wurden.
- Wenn Dateien in einer ReFS-Umgebung (ReFS = Resilient File System) zurückgeschrieben werden, werden Zurückschreibungen aus neueren Versionen von Windows Server in ältere Versionen nicht unterstützt, wie beispielsweise die Zurückschreibung einer Datei aus Windows Server 2016 in Windows Server 2012.
- Die Katalogisierung von Dateien, Sicherungen, Zurückschreibungen nach Zeitpunkt und andere Operationen, die den Windows-Agenten aufrufen, schlagen fehl, wenn ein anderer Administrator als der standardmäßige lokale Administrator bei **Benutzername für Gastbetriebssystem** beim Definieren eines Sicherungsjobs eingegeben wird. Ein Administrator, der nicht der standardmäßige lokale Administrator ist, ist jeder Benutzer, der im Gastbetriebssystem erstellt wurde und dem die Administratorrolle erteilt wurde.

  Dies ist der Fall, wenn der Registrierungsschlüssel `LocalAccountTokenFilterPolicy` in `[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]` auf 0 gesetzt oder nicht definiert wird. Wenn der Parameter auf 0 gesetzt oder nicht definiert wird, kann ein lokaler Administrator, der nicht der standardmäßige lokale Administrator ist, nicht mit WinRM interagieren; WinRM ist das Protokoll, das IBM Spectrum Protect Plus zum Installieren des Windows-Agenten für die Katalogisierung von Dateien, zum Senden von Befehlen an diesen Agenten und zum Abrufen von Ergebnissen von diesem Agenten verwendet.

  Setzen Sie den Registrierungsschlüssel `LocalAccountTokenFilterPolicy` auf der Windows-Gastmaschine, die mit aktivierter Option `Dateimetadaten katalogisieren` gesichert wird, auf 1. Wenn der Schlüssel nicht vorhanden ist, navigieren Sie zu `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]` und fügen Sie einen DWord-Registrierungsschlüssel mit dem Namen `LocalAccountTokenFilterPolicy` und dem Wert 1 hinzu.

Um Probleme zu verhindern, die aufgrund von Zeitzonendifferenzen auftreten können, verwenden Sie einen NTP-Server, um Zeitzonen ressourcenübergreifend zu synchronisieren. Sie können beispielsweise Zeitzonen für Speicherarrays, Hypervisoren und Anwendungsserver in Ihrer Umgebung synchronisieren.

Wenn die Zeitzonen nicht synchron sind, können während der Anwendungsregistrierung, dem Katalogisieren von Metadaten, Bestands-, Sicherungs-, Zurückschreibungs- oder Dateizurückschreibungsjobs Fehler auftreten. Weitere Informationen zum Identifizieren und Korrigieren von Zeitabweichungen finden Sie in Time in virtual machine drifts due to hardware timer drift.

Hinweise zu Hyper-V

Nur Datenträger auf SCSI-Platten sind für die Katalogisierung von Dateien und für die Dateizurückschreibung auswählbar.

Hinweise zu Linux

Wenn sich Daten auf LVM-Datenträgern befinden, muss der Service *lvm2-lvmetad* inaktiviert werden, da er die Fähigkeit von IBM Spectrum Protect Plus, Momentaufnahmen oder Klone der Datenträgergruppe bereitzustellen und erneut zu signieren, beeinträchtigen kann. Führen Sie die folgenden Schritte aus, um den Service zu inaktivieren:

1. Führen Sie die folgenden Befehle aus:

```
systemctl stop lvm2-lvmetad
```

```
systemctl disable lvm2-lvmetad
```

2. Editieren Sie `/etc/lvm/lvm.conf` und geben Sie die folgende Einstellung an:

```
use_lvmetad = 0
```

Wenn sich Daten auf XFS-Dateisystemen befinden und die Version des xfsprogs-Pakets zwischen 3.2.0 und 4.1.9 liegt, kann die Dateizurückschreibung aufgrund eines bekannten Problems in xfsprogs, das die Beschädigung eines Klon- oder Momentaufnahmedateisystems zur Folge hat, wenn seine UUID geändert wird, fehlschlagen. Aktualisieren Sie zur Lösung dieses Problems xfsprogs mit Version 4.2.0 oder höher. Weitere Informationen finden Sie in Debian Bug report logs.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Datei zurückzuschreiben.

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Dateizurückschreibung**.
2. Geben Sie einen Suchbegriff ein, um nach Namen nach einer Datei zu suchen, und klicken Sie dann auf das Suchsymbol  . Weitere Informationen zur Verwendung der Suchfunktion finden Sie in Anhang A, „Suchrichtlinien”, auf Seite 331.
3. Optional: Mithilfe von Filtern können Sie Ihre Suche in Bezug auf bestimmte virtuelle Maschinen, den Datumsbereich, in dem die Datei geschützt wurde, und die Betriebssystemtypen der virtuellen Maschinen optimieren.

   Suchvorgänge können über das Feld **Ordnerpfad** auch auf einen bestimmten Ordner beschränkt werden. Für das Feld **Ordnerpfad** werden Platzhalterzeichen unterstützt. Geben Sie Platzhalterzeichen am Anfang, in der Mitte oder am Ende einer Zeichenfolge an. Geben Sie beispielsweise `*Downloads` für eine Suche im Ordner `Downloads` ohne Angabe des vorhergehenden Pfads ein.
4. Um die Datei mithilfe der Standardoptionen zurückzuschreiben, klicken Sie auf **Zurückschreibung**. Die Datei wird an ihre ursprüngliche Position zurückgeschrieben.
5. Um Optionen zu editieren, bevor die Datei zurückgeschrieben wird, klicken Sie auf **Optionen**. Legen Sie die Dateizurückschreibungsoptionen fest.

   Vorhandene Dateien/Ordner überschreiben

   Ersetzen Sie die vorhandene Datei oder den vorhandenen Ordner durch die zurückgeschriebene Datei bzw. den zurückgeschriebenen Ordner.

   Ziel

   Wählen Sie diese Option aus, um die vorhandene Datei oder den vorhandenen Ordner durch die zurückgeschriebene Datei bzw. den zurückgeschriebenen Ordner zu ersetzen.

   Um die Datei an ihre ursprüngliche Position zurückzuschreiben, wählen Sie **Dateien in ursprüngliche Position zurückschreiben** aus.

   Um Daten an ein lokales Ziel zurückzuschreiben, das nicht mit der ursprünglichen Position übereinstimmt, wählen Sie **Dateien in alternative Position zurückschreiben** aus. Wählen Sie dann mithilfe

des Navigationsmenüs oder der Suchfunktion die alternative Position aus den verfügbaren Ressourcen aus.

Einschränkung: Eine Datei kann nur dann an eine alternative Position zurückgeschrieben werden, wenn für die alternative virtuelle Maschine über die Option **Benutzername/Kennwort für Gastbetriebssystem** in der Sicherungsjobdefinition Berechtigungsnachweise definiert wurden.

Geben Sie den Ordnerpfad der virtuellen Maschine am alternativen Ziel in das Feld **Zielordner** ein. Wenn das Verzeichnis nicht vorhanden ist, wird es erstellt.

Klicken Sie auf **Speichern**, um die Optionen zu speichern.

6. Um die Datei mithilfe definierter Optionen zurückzuschreiben, klicken Sie auf **Zurückschreibung**.

Zugehörige Tasks

„VMware-Daten sichern" auf Seite 107
Verwenden Sie einen Sicherungsjob, um VMware-Ressourcen, wie z. B. virtuelle Maschinen, Datenspeicher, Ordner, vApps und Datencenter, mit Momentaufnahmen zu sichern.

„VMware-Daten zurückschreiben" auf Seite 116
VMware-Zurückschreibungsjobs unterstützen Instant VM Restore- und Instant Disk Restore-Szenarios, die automatisch auf der Basis der ausgewählten Quelle erstellt werden.

Kapitel 8. Anwendungen schützen

Sie müssen die Datenbankanwendungen, die in IBM Spectrum Protect Plus geschützt werden sollen, registrieren und anschließend Jobs für die Sicherung und Zurückschreibung der Datenbanken und Ressourcen, die den Anwendungen zugeordnet sind, erstellen.

Anmerkung: IBM Spectrum Protect Plus kann Ordner auf Anwendungsservern erstellen, wenn Anwendungen in SPP registriert sind. Ordner, die von IBM Spectrum Protect Plus erstellt wurden, dürfen nicht entfernt werden, da das Produkt andernfalls nicht ordnungsgemäß funktioniert. Wenn ein von SSP erstellter Ordner entfernt werden muss, nehmen Sie die Registrierung der Anwendung in SPP zurück. SPP führt eine Bereinigung der Ordner durch, die der Registrierung zugeordnet sind.

Db2

Nachdem Sie Ihre IBM Db2-Instanzen in IBM Spectrum Protect Plus erfolgreich hinzugefügt haben, ist der Schutz Ihrer Db2-Daten möglich. Erstellen Sie SLA-Richtlinien (SLA = Service-Level-Agreement) zur Sicherung und Verwaltung von Db2-Daten.

Stellen Sie sicher, dass Ihre Db2-Umgebung die Systemanforderungen erfüllt. Weitere Informationen finden Sie in „Db2-Anforderungen" auf Seite 31.

Tipp: Wenn Ihre Db2-Daten in einer Umgebung mit mehreren Partitionen und mehreren Hosts gespeichert sind, können Sie Ihre Db2-Daten hostübergreifend schützen. Jeder Host in der Umgebung mit mehreren Partitionen muss IBM Spectrum Protect Plus hinzugefügt werden, sodass alle Instanzen und Datenbanken für den Schutz erkannt werden können. Weitere Informationen finden Sie in „Db2-Anwendungsserver hinzufügen" auf Seite 147.

Voraussetzungen für Db2

Alle Voraussetzungen für den IBM Spectrum Protect Plus Db2-Anwendungsserver müssen erfüllt sein, bevor Sie Db2-Ressourcen mit IBM Spectrum Protect Plus schützen.

Anforderungen für den IBM Spectrum Protect Plus Db2-Anwendungsserver sind in Db2-Anforderungen verfügbar.

Speichervoraussetzungen

Stellen Sie sicher, dass genügend Speicherbereich im Db2-Datenbankmanagementsystem, in den Datenträgergruppen für die Sicherungsoperation und auf den Zieldatenträgern vorhanden ist, um Dateien während der Zurückschreibungsoperation zu kopieren. Weitere Informationen zu Speicheranforderungen finden Sie in Speicheranforderungen für Db2-Schutz. Wenn Sie Daten an eine alternative Position zurückschreiben, ordnen Sie zusätzliche dedizierte Datenträger für die Kopier- und Zurückschreibungsprozesse zu. Die Datenpfade für Tabellenbereiche und Protokolle auf dem Zielhost sind mit den Pfaden auf dem ursprünglichen Host identisch. Diese Konfiguration ist erforderlich, damit Daten von dem bereitgestellten vSnap auf den Zielhost kopiert werden können. Stellen Sie sicher, dass dedizierte lokale Datenbankverzeichnisse für jede Datenbank in Ihrer Datenträgerkonfiguration zulässig sind.

Db2-Umgebungen mit mehrere Partitionen

Um Db2-Datenbanken mit mehreren Partitionen schützen zu können, muss für den ACS-Sicherungsmodus der parallele Modus festgelegt werden. Um die parallele Sicherungsverarbeitung von Partitionen in Ihrer Db2-Umgebung ausführen zu können, müssen Sie sicherstellen, dass eine der folgenden Voraussetzungen erfüllt ist:

© Copyright IBM Corp. 2017, 2019

- Die Db2-Registry-Variable **DB2_PARALLEL_ACS** ist auf YES gesetzt, beispielsweise **db2set DB2_PARALLEL_ACS=**YES.
- Die Db2-Registry-Variable **DB2_WORKLOAD** ist auf SAP gesetzt.

Einschränkung: Die Registry-Variable **DB2_PARALLEL_ACS** ist nur in bestimmten Fixpackstufen von Db2 verfügbar. Wenn **DB2_PARALLEL_ACS** in Ihrer Version nicht verfügbar ist, können Sie wahlweise **DB2_WORKLOAD** in SAP ändern.

Weitere Konfigurationsanforderungen

Stellen Sie sicher, dass Ihre Db2-Umgebung so konfiguriert ist, dass sie die folgenden Kriterien erfüllt:

- Die Db2-Archivprotokollierung ist aktiviert und Db2 befindet sich in einem wiederherstellbaren Modus.
- Db2-Tabellenbereiche sind von Protokolldateien getrennt und befinden sich jeweils auf dedizierten logischen Datenträgern, die von Linux Logical Volume Manager (LVM2) oder von AIX Journaling File System (JFS2) verwaltet werden.
- Stellen Sie sicher, dass die effektive Dateigröße **`ulimit`** -f für den IBM Spectrum Protect Plus-Agentenbenutzer und den Db2-Instanzbenutzer auf unlimited gesetzt ist. Es ist auch möglich, den Wert auf einen ausreichend hohen Wert zu setzen, der das Kopieren der größten Datenbankdateien in Ihren Sicherungs- und Zurückschreibungsjobs ermöglicht. Wenn Sie die Einstellung für **`ulimit`** ändern, starten Sie die Db2-Instanz erneut, um die Konfiguration abzuschließen.
- Wenn Sie IBM Spectrum Protect Plus in einer AIX- oder Linux-Umgebung ausführen, stellen Sie sicher, dass die installierte sudo-Version den empfohlenen Stand hat. Weitere Informationen finden Sie in Technote 2013790. Legen Sie dann sudo-Berechtigungen wie in „Sudo-Berechtigungen für Db2 definieren” auf Seite 146 beschrieben fest.
- Stellen Sie in einer Linux-Umgebung sicher, dass das Linux-Dienstprogrammpaket `util-linux-ng` oder das Paket `util-linux` aktuell ist.
- Stellen Sie sicher, dass der SSH-Service an Port 22 auf dem Server aktiv ist und Firewalls so konfiguriert sind, dass sie IBM Spectrum Protect Plus das Herstellen der Verbindung zum Server mit SSH ermöglichen. Das Subsystem SFTP für SSH muss aktiviert sein.
- Unicode-Zeichen in Dateipfadnamen können von IBM Spectrum Protect Plus nicht verarbeitet werden. Alle Namen müssen in ASCII codiert sein.
- Die Datenbanktabellenbereiche, Onlineprotokolle und das lokale Datenbankverzeichnis können sich auf einem einzigen dedizierten logischen Datenträger oder auf unterschiedlichen dedizierten logischen Datenträgern befinden, die von LVM2 oder JFS2 verwaltet werden. Die folgende Abbildung zeigt zwei Beispiele für das Layout. Die erste Abbildung zeigt zwei Typen von Datenträgergruppen. In der zweiten Abbildung befinden sich alle Datenträger für Daten und Protokolle in einer einzigen Datenträgergruppe.

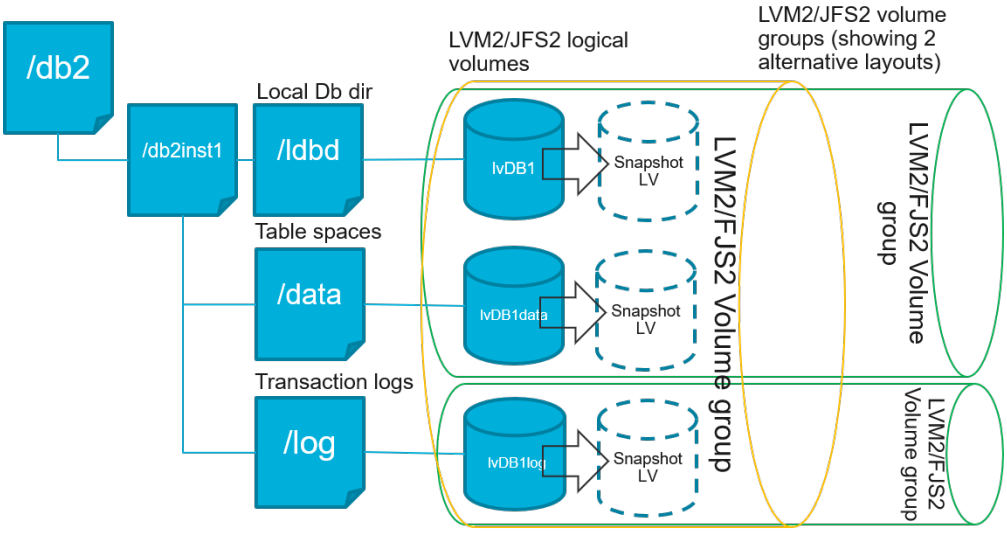


Abbildung 13. Beispiele für das Layout logischer Datenträger

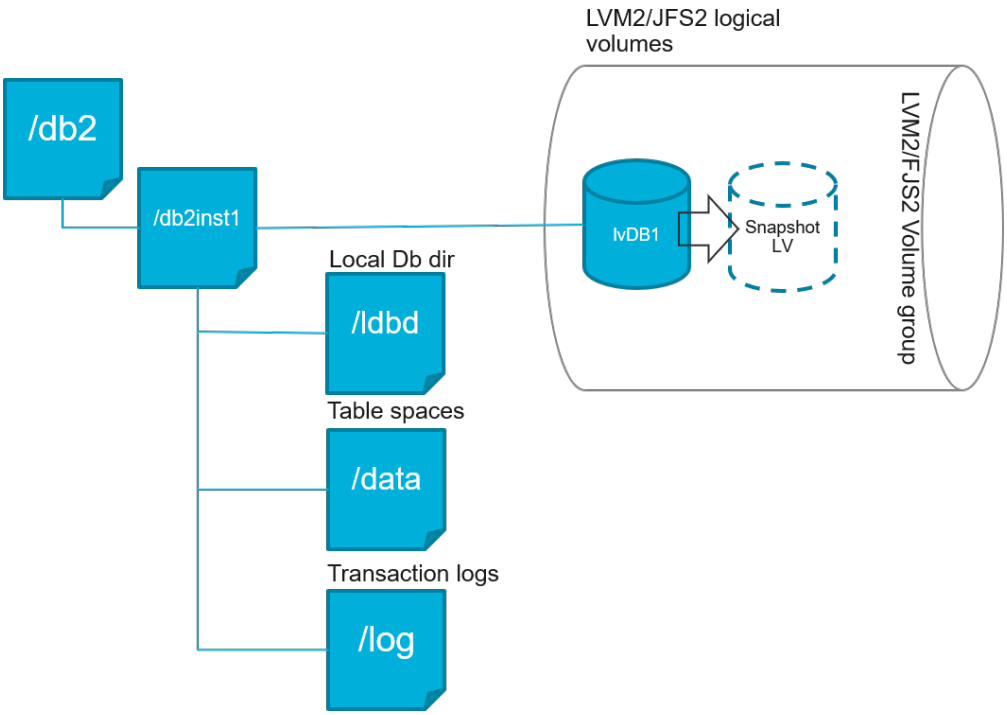


Abbildung 14. Beispiel für das Layout eines einzelnen logischen Datenträgers

- Stellen Sie sicher, dass die Konfiguration Ihrer logischen Datenträger in Db2 keine verschachtelten Mountpunkte enthält.

Speicheranforderungen für Db2-Schutz

Bevor Sie Db2-Datenbanken sichern, müssen Sie sicherstellen, dass genügend freier Plattenspeicherbereich auf den Ziel- und Quellenhosts und im vSnap-Repository vorhanden ist. Zusätzlicher freier Plattenspeicherbereich ist in den Datenträgergruppen auf dem Quellenhost erforderlich, um temporäre LVM-Momentaufnahmen der logischen Datenträger, auf denen die Db2-Datenbank und Protokolldateien gespeichert sind, erstellen zu können. Um LVM-Momentaufnahmen einer geschützten Db2-Datenbank zu erstellen, stellen Sie sicher, dass die Datenträgergruppen mit Db2-Daten über genügend freien Speicherbereich verfügen.

LVM-Momentaufnahmen

LVM-Momentaufnahmen sind Zeitpunktkopien logischer LVM-Datenträger. Sie sind platzsparende Momentaufnahmen mit den geänderten Datenaktualisierungen des logischen Quellendatenträgers. LVM-Momentaufnahmen werden in derselben Datenträgergruppe wie der logische Quellendatenträger erstellt. Der IBM Spectrum Protect Plus Db2-Agent verwendet LVM-Momentaufnahmen, um eine temporäre konsistente Zeitpunktkopie der Db2-Datenbank zu erstellen.

Der IBM Spectrum Protect Plus Db2-Agent erstellt eine LVM-Momentaufnahme, die dann bereitgestellt und in das vSnap-Repository kopiert wird. Die Dauer der Dateikopieroperation ist von der Größe der Db2-Datenbank abhängig. Während der Dateikopieroperation bleibt die Db2-Anwendung vollständig online. Nachdem die Dateikopieroperation beendet ist, werden die LVM-Momentaufnahmen vom IBM Spectrum Protect Plus Db2-Agenten in einer Bereinigungsoperation entfernt.

Bei AIX können maximal 15 Momentaufnahmen pro JFS2-Dateisystem vorhanden sein. Interne und externe JFS2-Momentaufnahmen können nicht gleichzeitig für dasselbe Dateisystem vorhanden sein. Stellen Sie sicher, dass keine internen Momentaufnahmen auf den JFS2-Datenträgern vorhanden sind, da diese Momentaufnahmen Probleme verursachen können, wenn der IBM Spectrum Protect Plus Db2-Agent externe Momentaufnahmen erstellt.

Für jeden logischen LVM- oder JFS2-Momentaufnahmedatenträger, der Daten enthält, müssen mindestens 10 Prozent seiner Größe als freier Plattenspeicherbereich in der Datenträgergruppe zulässig sein. Wenn die Datenträgergruppe über genügend freien Plattenspeicherbereich verfügt, reserviert der IBM Spectrum Protect Plus Db2-Agent bis zu 25 Prozent der Größe des logischen Quellendatenträgers für den logischen Momentaufnahmedatenträger.

LVM2 und JFS2
Wenn Sie eine Db2-Sicherungsoperation ausführen, fordert Db2 eine Momentaufnahme an. Diese Momentaufnahme wird auf einem Logical Volume Manager-System (LVM-System) oder einem Journaled File System (JFS) für jeden logischen Datenträger mit Daten oder Protokollen für die ausgewählte Datenbank erstellt. In Linux-Systemen werden die logischen Datenträger von LVM2 mit `lvm2`-Befehlen verwaltet. Unter AIX werden die logischen Datenträger von JFS2 verwaltet und mit dem JFS2-Momentaufnahmebefehl als externe Momentaufnahmen erstellt.

Eine softwarebasierte LVM2- oder JFS2-Momentaufnahme wird als neuer logischer Datenträger in derselben Datenträgergruppe erstellt. Die Momentaufnahmedatenträger werden vorübergehend auf derselben Maschine bereitgestellt, die die Db2-Instanz ausführt, sodass sie in das vSnap-Repository übertragen werden können.

Unter dem Betriebssystem Linux speichert der LVM2-Datenträgermanager die Momentaufnahme eines logischen Datenträgers in derselben Datenträgergruppe. Unter dem Betriebssystem AIX speichert der JFS2-Datenträgermanager die Momentaufnahme eines logischen Datenträgers in derselben Datenträgergruppe. In beiden Fällen muss auf der Maschine genügend Speicherbereich zum Speichern des logischen Datenträgers verfügbar sein. Die Größe des logischen Datenträgers nimmt in dem Maße zu, wie sich Daten auf dem Quellendatenträger während der Lebensdauer der Momentaufnahme ändern. In Umgebungen mit mehreren Partitionen wird, wenn mehrere Partitionen denselben Datenträger gemeinsam nutzen, für jede Partition eine zusätzliche Momentaufnahme des Datenträgers erstellt. Stellen Sie sicher, dass die Datenträgergruppe für die erforderlichen Momentaufnahmen über genügend freien Speicherbereich verfügt.

Sudo-Berechtigungen für Db2 definieren
Um IBM Spectrum Protect Plus zum Schutz Ihrer Daten zu verwenden, müssen Sie die erforderliche Version des sudo-Programms installieren. Für den Db2-Anwendungsserver müssen Sie sudo auf eine bestimmte Art und Weise definieren, die von der für andere Anwendungsserver abweichen kann.

Vorbereitende Schritte

Um die korrekte sudo-Version zu bestimmen, die installiert werden muss, lesen Sie die Informationen in Technote 2013790.

Informationen zu diesem Vorgang

Definieren Sie einen dedizierten IBM Spectrum Protect Plus-Agentenbenutzer mit den erforderlichen Superuserberechtigungen für sudo. Diese Konfiguration ermöglicht es dem Agentenbenutzer, Befehle ohne ein Kennwort auszuführen.

Vorgehensweise

1. Erstellen Sie einen Anwendungsserverbenutzer, indem Sie den folgenden Befehl ausgeben:

   ```
   useradd -m <Agent>
   ```

   Dabei gibt `Agent` den Namen des IBM Spectrum Protect Plus-Agentenbenutzers an.
2. Definieren Sie ein Kennwort für den neuen Benutzer, indem Sie den folgenden Befehl ausgeben:

   ```
   passwd <Agent>
   ```

3. Um Superuserberechtigungen für den Agentenbenutzer zu aktivieren, definieren Sie die Einstellung `!requiretty`. Fügen Sie am Ende der sudo-Konfigurationsdatei die folgenden Zeilen hinzu:

```
Defaults:<Agent> !requiretty
<Agent> ALL=(ALL) NOPASSWD:ALL
```

   Wenn Ihre sudoers-Datei für den Import von Konfigurationen aus einem anderen Verzeichnis (beispielsweise `/etc/sudoers.d`) konfiguriert ist, können Sie die Zeilen in der entsprechenden Datei in diesem Verzeichnis hinzufügen.

Db2-Anwendungsserver hinzufügen

Zum Schützen Ihrer Db2-Daten müssen Sie zunächst die Hostadresse hinzufügen, an der sich Ihre Db2-Instanzen befinden. Sie können die Prozedur wiederholen, um jeden Host hinzuzufügen, der mit IBM Spectrum Protect Plus geschützt werden soll. Wenn Ihre Db2-Umgebung mehrere Partitionen und mehrere Hosts enthält, müssen Sie IBM Spectrum Protect Plus jeden Host hinzufügen.

Informationen zu diesem Vorgang

Um IBM Spectrum Protect Plus einen Db2-Anwendungsserver hinzuzufügen, müssen Sie über die Hostadresse der Maschine verfügen.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **Db2**.
2. Klicken Sie im Fenster **Db2** auf **Anwendungsserver verwalten** und klicken Sie auf **Anwendungsserver hinzufügen**, um die Hostmaschine hinzuzufügen.

   Abbildung 15. Db2-Agent hinzufügen
3. Geben Sie im Abschnitt **Anwendungseigenschaften** die Hostadresse ein.
4. Wählen Sie aus, ob ein Benutzer angegeben oder ein SSH-Schlüssel verwendet werden soll.
   - Wenn Sie die Angabe eines Benutzers ausgewählt hatten, wählen Sie entweder einen vorhandenen Benutzer aus oder geben Sie eine Benutzer-ID und ein Kennwort ein.
   - Wenn Sie einen SSH-Schlüssel verwenden, wählen Sie den Schlüssel im Menü aus.

   Anmerkung: Für den Benutzer müssen sudo-Berechtigungen definiert sein.

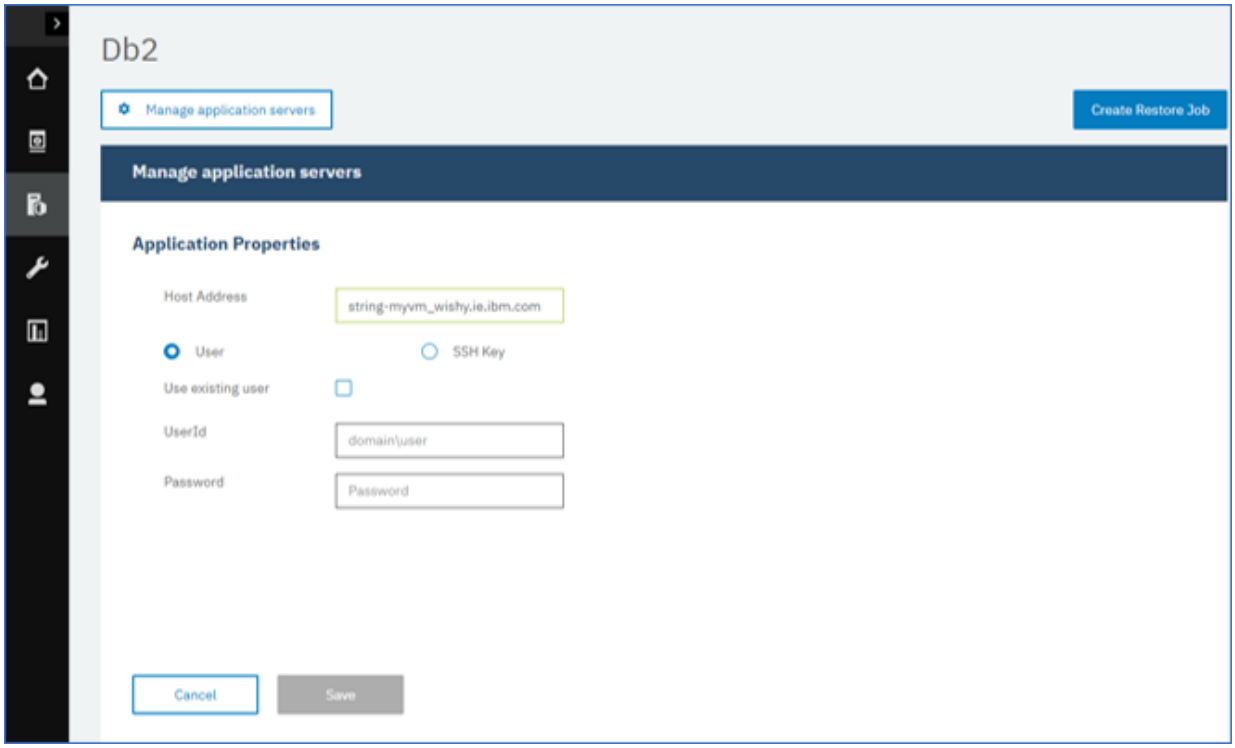


Abbildung 16. Agentenbenutzer verwalten

Tipp:

Die gefundenen Db2-Instanzen werden für jeden Host aufgelistet. Wenn Ihre Db2-Instanz partitioniert ist, wird diese Information mit der Hostmaschine und den Partitionsnummern aufgelistet. Bei DPF (Data Partitioning Feature) für mehrere Hosts wird die Db2-Instanz als eine einzige Einheit angezeigt.

5. Klicken Sie auf **Instanzen abrufen**, um die verfügbaren Db2-Instanzen aufzulisten.
6. Speichern Sie die Maske und wiederholen Sie die Schritte, um IBM Spectrum Protect Plus weitere Db2-Anwendungsserver hinzuzufügen.

   Wenn sich Ihre Db2-Daten in einer Umgebung mit mehreren Partitionen und mehreren Hosts befinden, müssen Sie jeden Host hinzufügen. Wiederholen Sie die Prozedur für jeden Db2-Host.

Nächste Schritte

Nachdem Sie IBM Spectrum Protect Plus Ihre Db2-Anwendungsserver hinzugefügt haben, wird automatisch auf jedem Anwendungsserver eine Bestandsverarbeitung ausgeführt, um die relevanten Datenbanken in diesen Instanzen zu erkennen.

Um zu verifizieren, ob die Datenbanken hinzugefügt wurden, überprüfen Sie das Jobprotokoll. Rufen Sie **Jobs und Operationen** auf. Klicken Sie auf die Registerkarte **Aktive Jobs** und suchen Sie nach dem neuesten Bestandsprotokolleintrag für den Anwendungsserver.

Beendete Jobs werden auf der Registerkarte **Jobprotokoll** angezeigt. Mithilfe der Liste **Sortieren nach** können Sie Jobs auf der Basis von Startzeit, Typ, Status, Jobnamen oder Dauer sortieren. Verwenden Sie das Feld **Nach Namen suchen**, um nach Jobs anhand des Namens zu suchen. Sie können Sterne als Platzhalterzeichen in dem Namen verwenden.

Datenbanken müssen erkannt werden, damit sie geschützt werden können. Anweisungen zur Ausführung einer Bestandsverarbeitung finden Sie in Db2-Ressourcen erkennen.

Db2-Ressourcen erkennen

Nachdem Sie IBM Spectrum Protect Plus IBM Db2-Anwendungsserver hinzugefügt haben, wird automatisch eine Bestandsverarbeitung ausgeführt, um alle Db2-Instanzen und -Datenbanken zu erkennen. Bei

der Bestandsverarbeitung werden alle Db2-Datenbanken für den ausgewählten Host erkannt, aufgelistet und gespeichert und die Datenbanken für den Schutz mit IBM Spectrum Protect Plus verfügbar gemacht.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie IBM Spectrum Protect Plus Ihre Db2-Anwendungsserver hinzugefügt haben. Anweisungen finden Sie in Db2-Anwendungsserver hinzufügen.

Informationen zu diesem Vorgang

Alle Db2-Partitionen, die im Bestand gefunden werden, werden für die Db2-Instanz aufgelistet. Die Partitionen werden nach ihrer Partitionsnummer für jeden Host in der Tabelle **Instanzen** aufgelistet; dabei wird die Partitionsnummer jeweils an den Hostnamen angefügt.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **Db2**.

   Tipp: Um dem Fenster **Instanzen** weitere Db2-Instanzen hinzuzufügen, führen Sie die Anweisungen in Db2-Anwendungsserver hinzufügen aus.
2. Klicken Sie auf **Bestandsverarbeitung ausführen**.

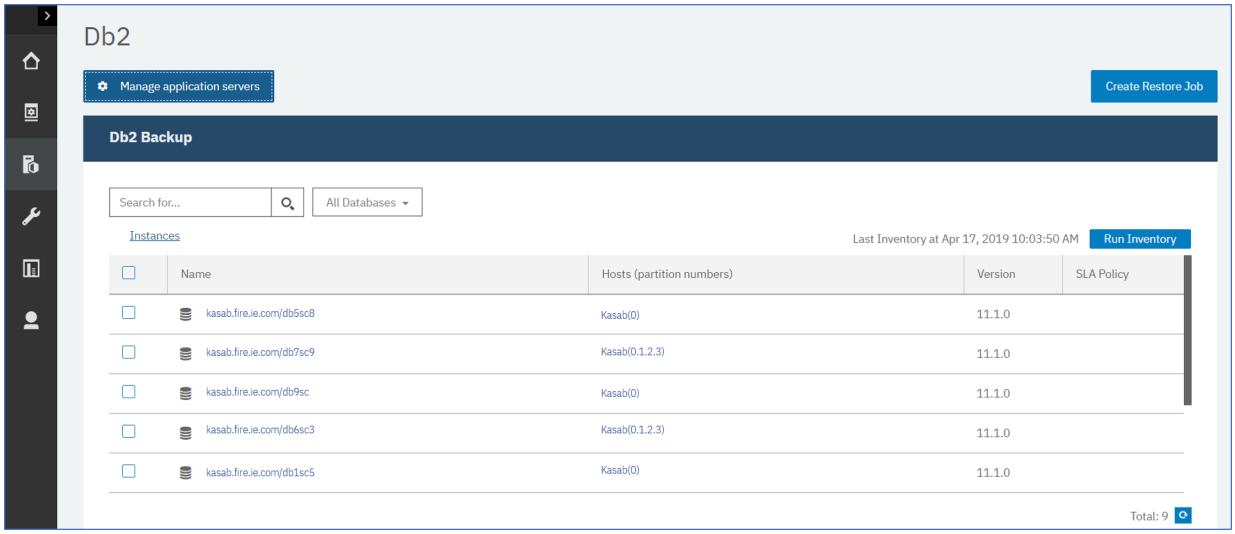


Abbildung 17. Db2-Ressourcen erkennen

Bei der Ausführung der Bestandsverarbeitung ändert sich die Schaltfläche und sie zeigt **Bestandsverarbeitung wird ausgeführt** an. Sie können eine Bestandsverarbeitung auf allen verfügbaren Anwendungsservern ausführen, Sie können jedoch nur jeweils einen einzigen Bestandsprozess ausführen.

Um das Jobprotokoll anzuzeigen, rufen Sie **Jobs und Operationen** auf. Klicken Sie auf die Registerkarte **Aktive Jobs** und suchen Sie nach dem neuesten Bestandsprotokolleintrag für den Anwendungsserver.

Beendete Jobs werden auf der Registerkarte **Jobprotokoll** angezeigt. Mithilfe der Liste **Sortieren nach** können Sie Jobs auf der Basis von Startzeit, Typ, Status, Jobnamen oder Dauer sortieren. Verwenden Sie das Feld **Nach Namen suchen**, um nach Jobs anhand des Namens zu suchen. Sie können Sterne als Platzhalterzeichen in dem Namen verwenden.

3. Klicken Sie auf eine Instanz, um eine Sicht zu öffnen, in der die für diese Instanz erkannten Datenbanken angezeigt werden. Wenn Datenbanken in der Liste **Instanzen** fehlen, überprüfen Sie Ihren Db2-Anwendungsserver und führen Sie den Bestandsjob erneut aus. In einigen Fällen sind bestimmte Datenbanken als nicht auswählbar für die Sicherung markiert; bewegen Sie den Mauszeiger über die Datenbank, um den Grund sichtbar zu machen.

Tipp: Um zur Liste der Instanzen zurückzukehren, klicken Sie auf den Hypertext **Instanzen** im Fenster **Db2-Sicherung**.

Nächste Schritte

Um die Db2-Datenbanken zu schützen, die in der ausgewählten Instanz katalogisiert sind, wenden Sie eine SLA-Richtlinie (SLA = Service-Level-Agreement) auf die Instanz an. Anweisungen zum Definieren einer SLA-Richtlinie finden Sie in SLA-Richtlinie definieren.

Db2-Verbindung testen

Nachdem Sie einen Db2-Anwendungsserver hinzugefügt haben, können Sie die Verbindung testen. Der Test verifiziert die Kommunikation mit dem Server und die DNS-Einstellungen zwischen IBM Spectrum Protect Plus und dem Db2-Server. Außerdem wird geprüft, ob die korrekten sudo-Berechtigungen für den Benutzer vorhanden sind.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Db2**.
2. Klicken Sie im Fenster **Db2** auf **Anwendungsserver verwalten** und wählen Sie die **Hostadresse** aus, die getestet werden soll.

   Eine Liste der verfügbaren Db2-Anwendungsserver wird angezeigt.
3. Klicken Sie auf **Aktionen** und wählen Sie **Testen** aus, um die Prüftests für physische Verbindungen, Fernverbindungen und Betriebssystemverbindungen und Einstellungen zu starten.

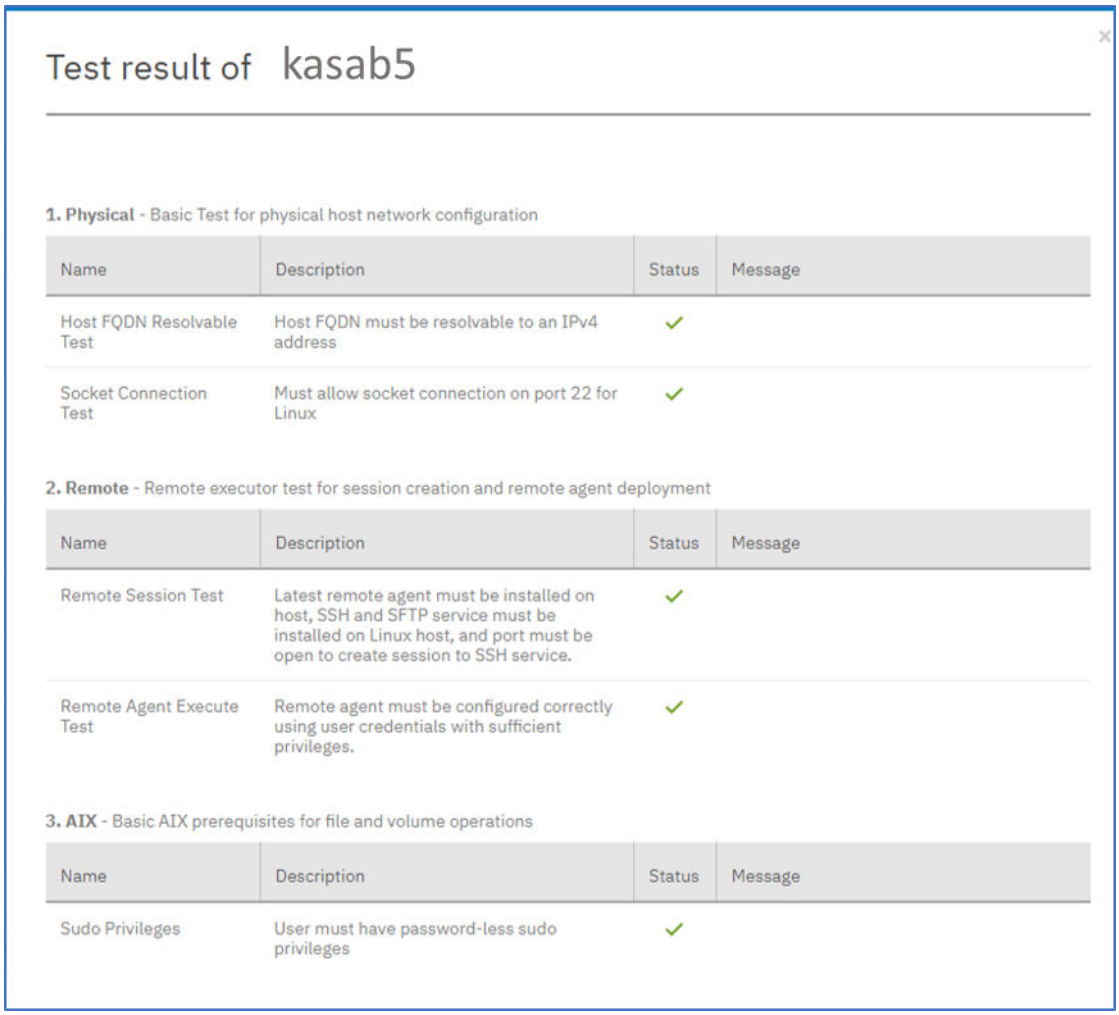


Abbildung 18. Verbindung testen

Der Testbericht zeigt eine Liste der Tests. Die Liste besteht aus einem Test für die Netzkonfiguration des physischen Hosts und aus einem Test für die Installation des fernen Servers auf dem Host, bei dem SSH und SFTP auf dem Host überprüft werden. Im dritten Test erfolgt eine Überprüfung auf die Betriebssystemvoraussetzungen und die korrekten sudo-Berechtigungen.

4. Klicken Sie auf **OK**, um den Test abzuschließen. Führen Sie den Test erneut aus, nachdem alle fehlgeschlagenen Tests korrigiert wurden.

Db2-Daten sichern

Definieren Sie regelmäßige Db2-Sicherungsjobs mit Optionen zum Ausführen und Erstellen von Sicherungskopien zum Schutz Ihrer Daten. Sie können die fortlaufende Sicherung von Archivprotokollen aktivieren, sodass Sie, falls erforderlich, eine Zeitpunktkopie mit Optionen für die aktualisierende Wiederherstellung zurückschreiben können.

Vorbereitende Schritte

Während der Erstsicherung erstellt IBM Spectrum Protect Plus einen neuen vSnap-Datenträger und eine neue NFS-Freigabe. Bei Teilsicherungen wird der zuvor erstellte Datenträger wiederverwendet. Der IBM Spectrum Protect Plus Db2-Agent stellt die Freigabe auf dem Db2-Server bereit, auf dem die Sicherung ausgeführt werden soll.

Lesen Sie die folgenden Prozeduren und Hinweise, bevor Sie eine Sicherungsjobdefinition erstellen:

- Fügen Sie die Anwendungsserver hinzu, die gesichert werden sollen. Die Prozedur finden Sie in Db2-Anwendungsserver hinzufügen.
- Konfigurieren Sie eine SLA-Richtlinie (SLA = Service Level Agreement). Die Prozedur finden Sie in SLA-Sicherungsjob definieren.
- Bevor ein IBM Spectrum Protect Plus-Benutzer Sicherungs- und Zurückschreibungsoperationen implementieren kann, müssen dem Benutzer Rollen und Ressourcengruppen zugeordnet werden. Erteilen Sie Benutzern mithilfe des Fensters **Accounts** Zugriff auf Ressourcen und Sicherungs- und Zurückschreibungsoperationen. Weitere Informationen finden Sie in Benutzerzugriff verwalten.
- Die Ausführung von Bestandsjobs sollte nicht gleichzeitig mit der Ausführung von Sicherungsjobs geplant werden.
- Vermeiden Sie die Konfiguration von Protokollsicherungen für eine einzelne Db2-Datenbank mit vielen Sicherungsjobs. Wenn eine einzelne Db2-Datenbank mehreren Jobdefinitionen mit aktivierter Protokollsicherung hinzugefügt wird, kann eine Protokollsicherung von einem Job ein Protokoll abschneiden, bevor es vom nächsten Job gesichert wird. Dies kann zur Folge haben, dass Jobs für Zurückschreibungen nach Zeitpunkt fehlschlagen.

Vorgehensweise

1. Erweitern Sie im Navigationsmenü **Schutz verwalten** > **Anwendungen** > **Db2**.
2. Wählen Sie eine Instanz oder Datenbank zum Sichern aus, indem Sie eine der folgenden Aktionen auswählen:
   - Wählen Sie eine vollständige Instanz im Fenster **Instanzen** aus, indem Sie auf das Kontrollkästchen neben dem Instanznamen klicken. Alle Datenbanken, die dieser Instanz hinzugefügt wurden, werden automatisch der SLA-Richtlinie zugeordnet, die Sie auswählen.
   - Wählen Sie eine bestimmte Datenbank in einer Instanz aus, indem Sie auf den Instanznamen klicken und eine Datenbank aus der Liste der Datenbanken in dieser Instanz auswählen.

   Jeder Eintrag im Fenster **Instanzen** wird nach dem Instanz- oder Datenbanknamen, der angewendeten SLA-Richtlinie und der Wählbarkeit für die Protokollsicherung aufgelistet.
3. Klicken Sie auf **Optionen auswählen**, um die Protokollsicherung zu aktivieren oder zu inaktivieren und parallele Datenströme anzugeben, mit denen der Zeitaufwand für eine große Datenversetzung in der Sicherungsoperation minimiert werden soll. Klicken Sie auf **Speichern**, um die Optionen festzuschreiben.

Wählen Sie **Protokollsicherung aktivieren** aus, um Archivprotokolle zu sichern; dies ermöglicht die Angabe von Optionen für die Zurückschreibung nach Zeitpunkt und von Wiederherstellungsoptionen. Informationen zu den Einstellungen für Db2-Protokollsicherungen finden Sie in Protokollsicherungen.

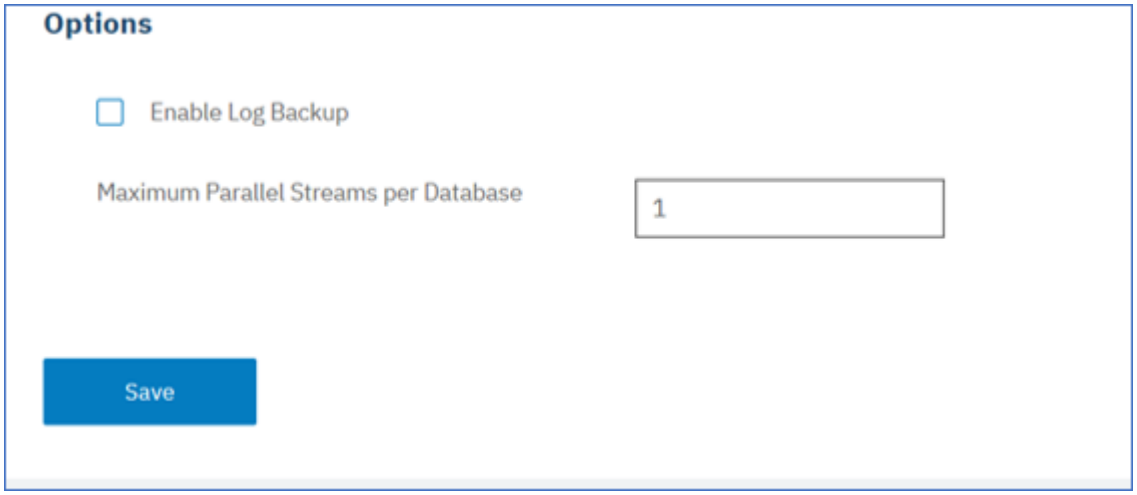


Abbildung 19. Fenster "Sicherung" mit der Option "Protokollsicherung aktivieren"

Wenn Sie die Optionen speichern, werden diese Optionen für alle Sicherungsjobs für die ausgewählte Datenbank oder Instanz verwendet.

4. Wählen Sie die Datenbank oder Instanz erneut aus und klicken Sie auf **SLA-Richtlinie auswählen**, um eine SLA-Richtlinie für diese Datenbank oder Instanz auszuwählen.
5. Speichern Sie die SLA-Optionen.

   Um eine neue SLA-Richtlinie zu definieren oder eine vorhandene Richtlinie mit angepassten Raten für die Aufbewahrung und Häufigkeit zu editieren, wählen Sie **Schutz verwalten** > **Richtlinienübersicht** aus. Klicken Sie im Fenster **SLA-Richtlinien** auf **SLA-Richtlinie hinzufügen** und definieren Sie Ihre Richtlinienvorgaben.

Nächste Schritte

Wenn die SLA-Richtlinie gespeichert wird, können Sie zu jeder Zeit eine bedarfsgesteuerte Sicherung ausführen, indem Sie auf **Aktionen** neben dem Richtliniennamen klicken und **Starten** auswählen. Der Status im Protokoll ändert sich, um anzuzeigen, dass die Sicherung `Aktiv` ist.

SLA-Sicherungsjob definieren

Nachdem Ihre Db2-Datenbanken für alle Ihre Db2-Instanzen aufgelistet wurden, wählen Sie eine SLA-Richtlinie (SLA = Service-Level-Agreement) aus und wenden Sie die Richtlinie an, um Ihre Daten zu schützen.

Vorgehensweise

1. Erweitern Sie im Navigationsmenü **Schutz verwalten** > **Anwendungen** > **Db2**.
2. Wählen Sie eine Db2-Instanz aus, um alle Daten in dieser Instanz zu sichern, oder klicken Sie auf den Instanznamen, um die für die Sicherung verfügbaren Datenbanken anzuzeigen. Sie können dann einzelne Datenbanken, die gesichert werden sollen, in der Db2-Instanz auswählen.

   Wahlweise können Sie eine vollständige Instanz mit allen zugeordneten Daten oder eine oder mehrere Datenbanken sichern.

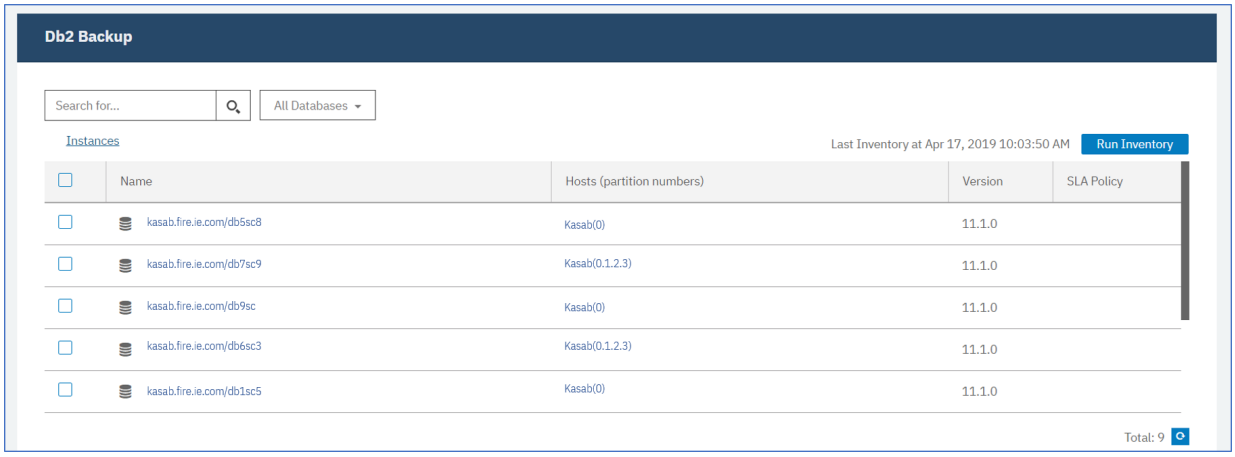


Abbildung 20. Fenster "Db2-Sicherung" mit Instanzen

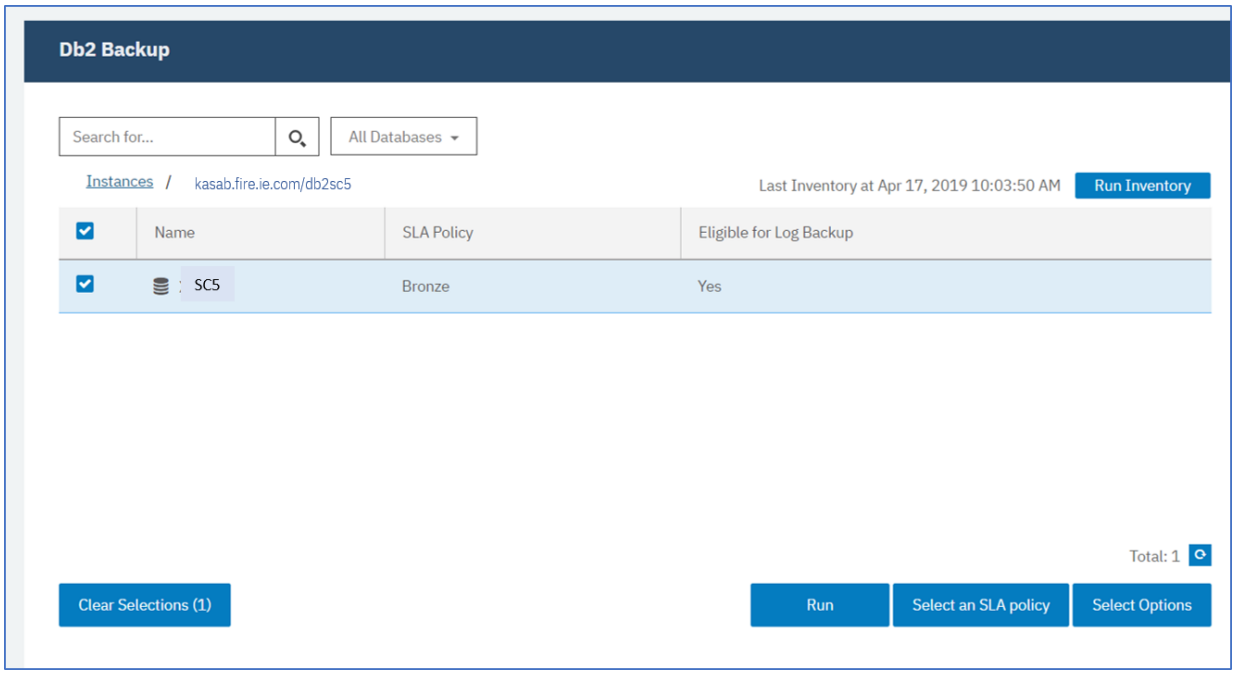


Abbildung 21. Fenster "Db2-Sicherung" mit Datenbanken in einer Instanz

3. Klicken Sie auf **SLA-Richtlinie auswählen** und wählen Sie eine SLA-Richtlinie (**Gold**, **Silber** oder **Bronze**) aus. Speichern Sie Ihre Auswahl.

   Die vordefinierten Auswahlmöglichkeiten "Gold", "Silber" und "Bronze" verfügen über verschiedene Häufigkeiten und Aufbewahrungsraten. Sie können eine angepasste SLA-Richtlinie erstellen oder eine vorhandene Richtlinie editieren, indem Sie zu **Richtlinienübersicht** > **SLA-Richtlinien** navigieren.
4. Klicken Sie auf **Optionen auswählen**, um Optionen für Ihre Sicherung zu definieren, wie z. B. Aktivierung von Protokollsicherungen für zukünftige Wiederherstellungsoptionen und Angabe der Anzahl paralleler Datenströme, um den Zeitaufwand für die Sicherung großer Datenbanken zu reduzieren. Speichern Sie Ihre Änderungen.

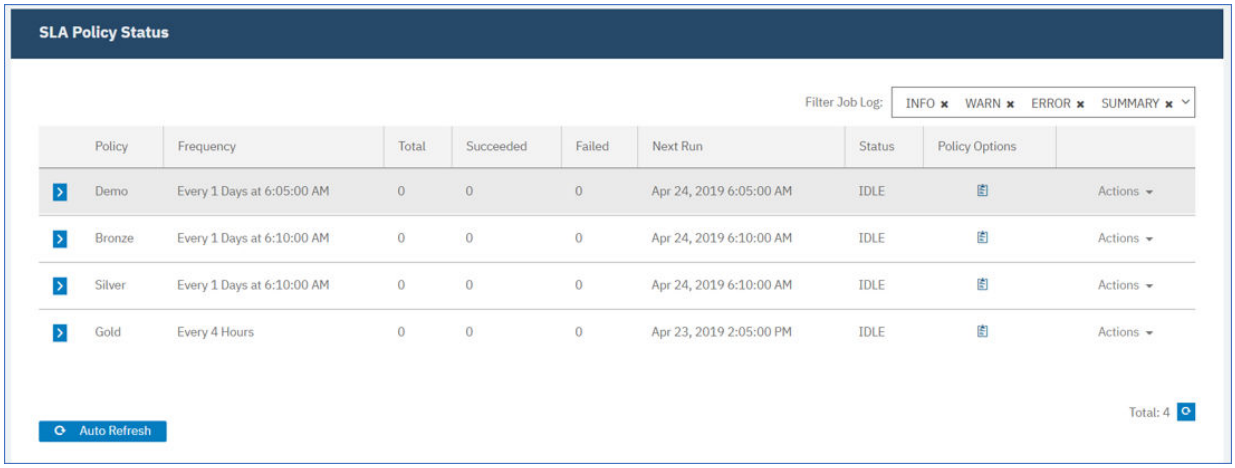


Abbildung 22. Sicherungsoptionen und SLA-Richtlinien

5. Konfigurieren Sie die SLA-Richtlinie, indem Sie auf das Symbol in der Spalte **Richtlinienoptionen** der Tabelle **SLA-Richtlinienstatus** klicken.

   Informationen zu weiteren SLA-Konfigurationsoptionen finden Sie in „SLA-Konfigurationsoptionen für einen Sicherungsjob definieren" auf Seite 154.
6. Soll die Richtlinie außerhalb des geplanten Jobs ausgeführt werden, wählen Sie die Instanz oder Datenbank aus. Klicken Sie auf **Aktionen** und wählen Sie **Starten** aus.

   Der Status für die ausgewählte SLA-Richtlinie wird in **Aktiv** geändert, und Sie können den Fortschritt des Jobs im angezeigten Jobprotokoll verfolgen.

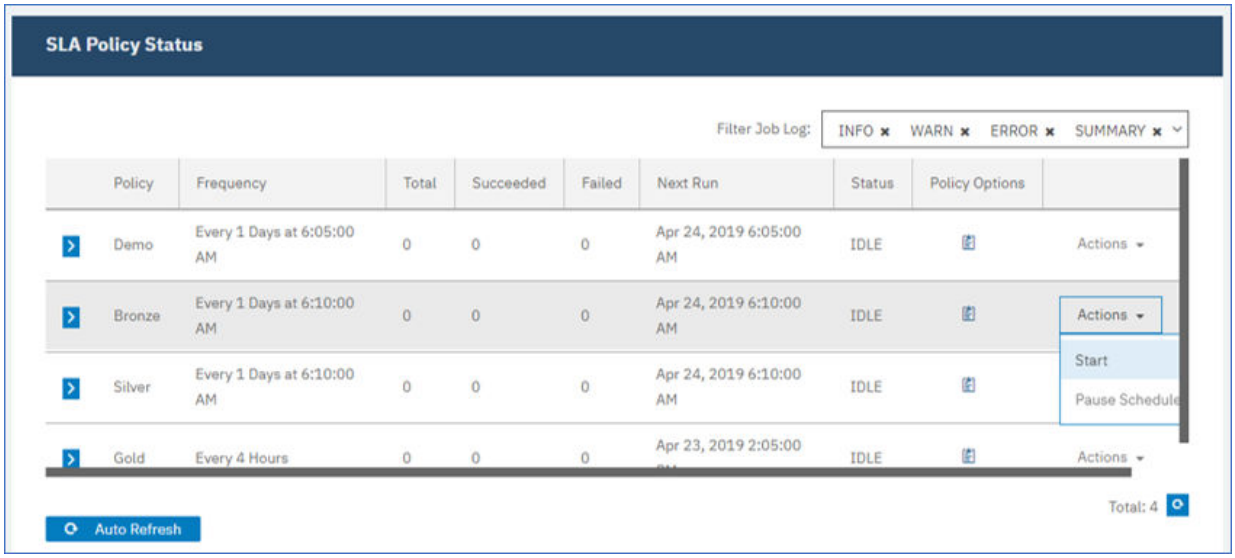


Abbildung 23. SLA-Richtlinien

Um den Zeitplan eines SLA anzuhalten, klicken Sie auf **Aktionen** und wählen Sie **Zeitplan anhalten** aus.

Um einen Job nach seinem Start abzubrechen, klicken Sie auf **Aktionen** > **Abbrechen**.

SLA-Konfigurationsoptionen für einen Sicherungsjob definieren

Nachdem Sie ein Service-Level-Agreement (SLA) für Ihren Sicherungsjob definiert haben, können Sie weitere Optionen für diesen Job konfigurieren. Sie können Scripts ausführen, Ressourcen von der Sicherungsoperation ausschließen und bei Bedarf eine vollständige Basissicherungskopie einer Datenbank erzwingen.

Vorgehensweise

1. Klicken Sie in der Spalte **Richtlinienoptionen** der Tabelle **SLA-Richtlinienstatus** für den Job, den Sie konfigurieren, auf das Zwischenablagesymbol , um zusätzliche Konfigurationsoptionen anzugeben. Ist der Job bereits konfiguriert, klicken Sie auf das Symbol, um die Konfiguration zu editieren.

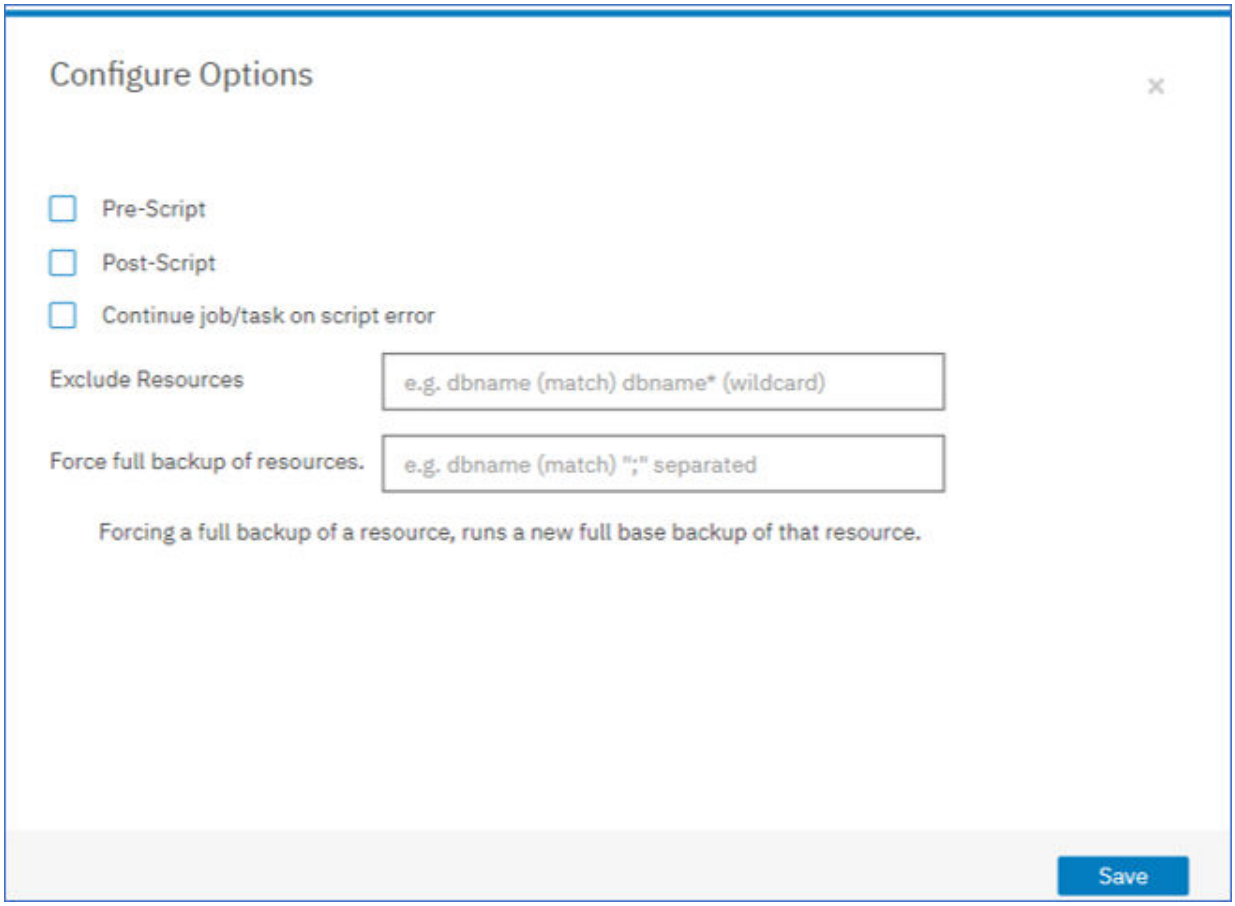


Abbildung 24. SLA-Konfigurationsoptionen angeben

2. Klicken Sie auf **Vorscript** und definieren Sie Ihre Vorscriptkonfiguration, indem Sie eine der folgenden Optionen auswählen:
   - Klicken Sie auf **Scriptserver verwenden** und wählen Sie ein hochgeladenes Script aus dem Menü aus.
   - Klicken Sie nicht auf **Scriptserver verwenden**. Wählen Sie einen Anwendungsserver aus der Liste aus, um das Script an dieser Position auszuführen.
3. Klicken Sie auf **Nachscript** und definieren Sie Ihre Nachscriptkonfiguration, indem Sie eine der folgenden Optionen auswählen:
   - Klicken Sie auf **Scriptserver verwenden** und wählen Sie ein hochgeladenes Script aus dem Menü aus.
   - Klicken Sie nicht auf **Scriptserver verwenden**. Wählen Sie einen Anwendungsserver aus der Liste aus, um das Script an dieser Position auszuführen.

   Scripts und Scriptserver werden auf der Seite **Systemkonfiguration** > **Script** konfiguriert. Weitere Informationen zum Arbeiten mit Scripts finden Sie in Scripts konfigurieren.
4. Um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt, wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus.

Wenn diese Option ausgewählt wird und das Script die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird erneut versucht, die Sicherungs- oder Zurückschreibungsoperation auszuführen, und der Taskstatus des Scripts wird als ABGESCHLOSSEN zurückgemeldet. Wenn diese Option nicht ausgewählt wird, wird nicht erneut versucht, die Sicherung oder Zurückschreibung auszuführen, und der Taskstatus des Scripts wird als FEHLGESCHLAGEN zurückgemeldet.

5. Um Ressourcen von einem Sicherungsjob auszuschließen, geben Sie die Ressourcen an, die von dem Job ausgeschlossen werden sollen. Geben Sie einen genauen Ressourcennamen in das Feld **Ressourcen ausschließen** ein. Wenn Sie sich bezüglich eines Namens nicht sicher sind, verwenden Sie Sterne als Platzhalterzeichen, die vor dem Muster (**text*) oder hinter dem Muster (*text**) angegeben werden. Mehrere Platzhalterzeichen können mit alphanumerischen Standardzeichen und den folgenden Sonderzeichen eingegeben werden: - _ und *. Trennen Sie Einträge durch ein Semikolon voneinander.
6. Um eine neue Gesamtsicherung einer Ressource zu erstellen, geben Sie den Namen dieser Ressource in das Feld **Gesamtsicherung der Ressourcen erzwingen** ein. Trennen Sie mehrere Ressourcen durch ein Semikolon voneinander.

   Bei der Gesamtsicherung wird einmalig eine neue Gesamtsicherung dieser Ressource erstellt und die vorhandene Sicherung dieser Ressource ersetzt. Nach Abschluss der Gesamtsicherung wird die Ressource wie zuvor mit Teilsicherungen gesichert.

Protokollsicherungen
Archivierte Protokolle für Datenbanken enthalten festgeschriebene Transaktionsdaten. Diese Transaktionsdaten können zur Ausführung einer aktualisierenden Datenwiederherstellung verwendet werden, wenn Sie eine Zurückschreibungsoperation ausführen. Durch die Verwendung von Archivprotokollsicherungen wird die Zielsetzung für Wiederherstellungspunkt für Ihre Daten verbessert.

Stellen Sie sicher, dass Sie die Option **Protokollsicherung aktivieren** auswählen, um die aktualisierende Wiederherstellung zu ermöglichen, wenn Sie einen Sicherungsjob oder eine SLA-Richtlinie konfigurieren. Beim ersten Auswählen müssen Sie einen Sicherungsjob für die SLA-Richtlinie ausführen, um die Protokollarchivierung in IBM Spectrum Protect Plus in der Datenbank zu aktivieren. Mit dieser Sicherung wird im vSnap-Repository ein separater Datenträger erstellt, der permanent auf dem Db2-Anwendungsserver bereitgestellt wird. Der Sicherungsprozess aktualisiert entweder den Parameter **LOGARCHMETH1** oder den Parameter **LOGARCHMETH2** so, dass er für Protokollarchivierungszwecke auf diesen Datenträger verweist. Der Datenträger bleibt auf dem Db2-Anwendungsserver bereitgestellt, es sei denn, die Option **Protokollsicherung aktivieren** wird abgewählt und ein neuer Sicherungsjob ausgeführt.

Einschränkung: In Db2-Umgebungen mit mehreren Partitionen müssen die **LOGARCHMETH**-Parameter in allen Partitionen übereinstimmen.

Wenn entweder für den Parameter **LOGARCHMETH1** oder für den Parameter **LOGARCHMETH2** ein anderer Wert als OFF festgelegt ist, können Sie archivierte Protokolle für die aktualisierende Wiederherstellung verwenden. Sie können Protokollsicherungsjobs jederzeit abbrechen, indem Sie die Option **Protokollsicherung aktivieren** abwählen: Rufen Sie **Schutz verwalten** > **Anwendungen** > **Db2** auf, wählen Sie die Instanz aus und klicken Sie auf **Optionen auswählen**. Diese Änderung wird Anschluss an den nächsten erfolgreich ausgeführten Sicherungsjob wirksam; der Wert des **LOGARCHMETH**-Parameters wird wieder in seine ursprüngliche Einstellung geändert.

Wichtig: IBM Spectrum Protect Plus kann Protokollsicherungsjobs nur aktivieren, wenn der Parameter **LOGARCHMETH1** auf LOGRETAIN gesetzt ist oder wenn einer der **LOGARCHMETH**-Parameter auf OFF gesetzt ist.

Wenn der Parameter LOGARCHMETH1 auf LOGRETAIN gesetzt ist

IBM Spectrum Protect Plus ändert den Wert des Parameters **LOGARCHMETH1**, um Protokollsicherungen zu aktivieren.

Wenn entweder der Parameter LOGARCHMETH1 oder der Parameter LOGARCHMETH2 auf OFF gesetzt ist und der andere Parameter auf DISK, TSM oder VENDOR gesetzt ist

IBM Spectrum Protect Plus verwendet den **LOGARCHMETH**-Parameter, der auf OFF gesetzt ist, um Protokollsicherungen zu aktivieren.

Wenn beide LOGARCHMETH-Parameter auf DISK, TSM oder VENDOR gesetzt sind
Diese Einstellung hat einen Fehler zur Folge, wenn IBM Spectrum Protect Plus versucht, Protokollsicherungen zu aktivieren. Um den Fehler zu beheben, setzen Sie einen der Parameter auf OFF und führen Sie den Sicherungsjob mit ausgewählter Option **Protokollsicherung aktivieren** aus.

Archivprotokollsicherungen abschneiden

IBM Spectrum Protect Plus löscht ältere Transaktionsprotokolle automatisch nach einer erfolgreichen Datenbanksicherung. Mit dieser Aktion wird sichergestellt, dass die Kapazität des Protokollarchivdatenträgers durch die Aufbewahrung älterer Protokolldateien nicht beeinträchtigt wird. Diese abgeschnittenen Protokolldateien werden so lange im vSnap-Repository gespeichert, bis die zugehörige Sicherung verfällt und gelöscht wird. Die Aufbewahrung von Datenbanksicherungen ist in der von Ihnen ausgewählten SLA-Richtlinie definiert. Weitere Informationen zu SLA-Richtlinien finden Sie in „SLA-Sicherungsjob definieren” auf Seite 152.

IBM Spectrum Protect Plus verwaltet nicht die Aufbewahrung anderer Archivprotokollpositionen.

Weitere Informationen zu Db2-Einstellungen finden Sie auf der IBM Db2-Begrüßungsseite.

Db2-Daten zurückschreiben

Um Db2-Daten aus dem vSnap-Repository zurückzuschreiben, definieren Sie einen Job, der Daten entweder aus der neuesten Sicherung oder aus einer früheren Sicherungskopie zurückschreibt. Sie können Daten wahlweise in die ursprüngliche Instanz oder in eine alternative Instanz auf einer anderen Maschine zurückschreiben, Wiederherstellungsoptionen angeben und den Job speichern.

Vorbereitende Schritte

Wichtig: Für alle Zurückschreibungsoperationen muss Db2 auf den Quellen- und Zielhosts denselben Versionsstand haben. Zusätzlich zu dieser Anforderung müssen Sie sicherstellen, dass auf jedem Host eine Instanz vorhanden ist, die denselben Namen wie die Instanz hat, die zurückgeschrieben wird. Diese Anforderung gilt, wenn die Zielinstanz denselben Namen hat und wenn die Namen unterschiedlich sind. Damit die Zurückschreibungsoperation erfolgreich ausgeführt werden kann, müssen beide Instanzen bereitgestellt werden, eine mit dem ursprünglichen Namen und die andere mit dem neuen Namen.

Wenn Ihre Db2-Umgebung partitionierte Datenbanken umfasst, werden die Daten aller Partitionen während der regelmäßigen Sicherungsjobs gesichert. Alle Instanzen werden im Fenster "Sicherung" aufgelistet. Instanzen mit mehreren Partitionen werden mit Partitionsnummern und Hostnamen angezeigt.

Bevor Sie einen Zurückschreibungsjob für Db2 erstellen, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Mindestens ein Db2-Sicherungsjob ist definiert und wird erfolgreich ausgeführt. Anweisungen zum Definieren eines Sicherungsjobs finden Sie in „Db2-Daten sichern” auf Seite 151.
- IBM Spectrum Protect Plus-Rollen und -Ressourcengruppen sind dem Benutzer zugeordnet, der den Zurückschreibungsjob definiert. Weitere Informationen zum Zuordnen von Rollen finden Sie in Kapitel 13, „Benutzerzugriff verwalten”, auf Seite 311.
- Bei einer Zurückschreibung aus einem IBM Spectrum Protect-Archiv werden Dateien vom Band in einen Staging-Pool migriert, bevor der Job gestartet wird. Abhängig von der Größe der Zurückschreibung kann dieser Prozess mehrere Stunden dauern.

Anmerkung: Wenn Sie Datenbanken mit mehreren Partitionen an eine alternative Position zurückschreiben, stellen Sie sicher, dass die Zielinstanz mit denselben Partitionsnummern wie die ursprüngliche Instanz konfiguriert ist. Alle diese Partitionen müssen sich auf einem einzigen Host befinden. Wenn Daten in eine neue Instanz zurückgeschrieben werden, die umbenannt wird, müssen beide Instanzen, die für die Zurückschreibungsoperation erforderlich sind, mit derselben Anzahl Partitionen konfiguriert werden.

Bevor Sie eine Operation zum Zurückschreiben in eine alternative Instanz starten, stellen Sie sicher, dass die Dateisystemstruktur auf der Quellenmaschine mit der auf der Zielmaschine übereinstimmt. Diese Dateisystemstruktur umfasst Tabellenbereiche, Onlineprotokolle und das lokale Datenbankverzeichnis. Stel-

len Sie sicher, dass dedizierte Datenträger mit genügend Speicherbereich der Dateisystemstruktur zugeordnet werden. Db2 muss für alle Zurückschreibungsoperationen über denselben Versionsstand auf dem Quellen- und dem Zielhost verfügen und eine Instanz mit demselben Namen muss auf jedem Host vorhanden sein. Weitere Informationen zu den Speicheranforderungen finden Sie in Speicheranforderungen für Db2-Schutz. Weitere Informationen zu den Voraussetzungen und zur Konfiguration finden Sie in Voraussetzungen für Db2.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **Db2** und klicken Sie auf **Zurückschreibungsjob erstellen**.

   Der Assistent "Momentaufnahmezurückschreibung" wird geöffnet.
2. Optional: Wenn der Zurückschreibungsassistent über die Seite **Jobs und Operationen** gestartet wurde, wählen Sie Db2 als den Quellentyp aus und klicken Sie auf **Weiter**.

   Tipp: Um eine Zusammenfassung Ihrer Auswahlangaben im Zurückschreibungsassistenten zu erhalten, bewegen Sie den Cursor im Navigationsfenster des Assistenten auf das Informationssymbol .
3. Klicken Sie auf der Seite **Quellenauswahl** auf eine Db2-Instanz, um die Datenbanken in dieser Instanz anzuzeigen. Wählen Sie eine Datenbank aus, indem Sie auf das Plussymbol neben dem Datenbanknamen klicken. Klicken Sie auf **Weiter**, um fortzufahren.
4. Wählen Sie auf der Seite **Quellenmomentaufnahme** den Typ der erforderlichen Zurückschreibungsoperation aus.

   - **Bedarfsgesteuert: Momentaufnahme**: Erstellt eine einmalige Zurückschreibungsoperation aus einer Datenbankmomentaufnahme. Der Job wird nicht als sich wiederholender Job definiert.
   - **Bedarfsgesteuert: Zeitpunkt**: Erstellt eine einmalige Zurückschreibungsoperation aus einer Sicherung der Datenbank nach Zeitpunkt. Der Job wird nicht als sich wiederholender Job definiert.
   - **Wiederholt auftretend**: Erstellt einen sich wiederholenden Job, der gemäß einem Zeitplan ausgeführt wird und wiederholt ausgeführt wird.

   Tipp:

   Für **Bedarfsgesteuert: Momentaufnahme** können Sie "Keine Wiederherstellung" oder "Bis zum Ende der Sicherung wiederherstellen" auswählen. Für einen Zurückschreibungsjob des Typs **Bedarfsgesteuert: Zeitpunkt** können Sie "Bis zum Ende der verfügbaren Protokolle wiederherstellen" oder "Bis zu einem bestimmten Zeitpunkt wiederherstellen" auswählen.
5. Wählen Sie auf derselben Seite wie folgt einen **Typ der Zurückschreibungsposition** aus:

Position	Anweisungen
Site	Wählen Sie diese Option aus, um Daten von der primären oder sekundären Site zurückzuschreiben. "Site" ist die einzige Auswahl für bedarfsgesteuerte Zurückschreibungsjobs nach Zeitpunkt.
Cloudauslagerung	Wählen Sie diese Option aus, um Daten aus Cloudspeicher zurückzuschreiben. Geben Sie den Zurückschreibungspunkt an, der für die Momentaufnahme verwendet werden soll.
Repository-Auslagerung	Wählen Sie diese Option aus, um Daten aus einem vSnap-Repository zurückzuschreiben. Geben Sie den Zurückschreibungspunkt an, der für die Momentaufnahme verwendet werden soll.
Cloudarchivierung	Wählen Sie diese Option aus, um Daten zurückzuschreiben, die in der Cloud archiviert sind. Geben Sie den Zurückschreibungspunkt an, der für die Momentaufnahme verwendet werden soll.

Position	Anweisungen
Repository-Archivierung	Wählen Sie diese Option aus, um Daten zurückzuschreiben, die im vSnap-Repository archiviert sind. Geben Sie den Zurückschreibungspunkt an, der für die Momentaufnahme verwendet werden soll.

Wenn Sie eine bedarfsgesteuerte Momentaufnahme erstellen, können Sie für die Momentaufnahme, nach der gesucht wird, einen Zeitraum angeben. Soweit zutreffend können Sie einen anderen vSnap-Server für die Operation verwenden.

6. Wählen Sie eine Position für die Zurückschreibungsoperation aus. Wählen Sie eine der folgenden Optionen für die Position aus und klicken Sie auf **Weiter**.

Option	Bezeichnung
Demo	Wählen Sie diese Option aus, um Daten vom vSnap-Demonstrationsserver zurückzuschreiben. Diese Option ist nur in bestimmten Konfigurationen verfügbar.
Primär	Wählen Sie diese Option aus, um Daten aus dem primären vSnap-Server an das Ziel zurückzuschreiben. Diese Position ist für den Zurückschreibungspositionstyp Site verfügbar.
Sekundär	Wählen Sie diese Option aus, um Daten aus dem sekundären vSnap-Server an das Ziel zurückzuschreiben. Diese Position ist für den Zurückschreibungspositionstyp Site verfügbar.

Zurückschreibungspunkte sind über das Menü **Zurückschreibungspunkt** verfügbar.

7. Wählen Sie eine für das für die Zurückschreibungsoperation ausgewählte Ziel geeignete **Zurückschreibungsmethode** aus. Klicken Sie auf **Weiter**, um fortzufahren.

   - **Instant Access**: In diesem Modus wird keine weitere Aktion ausgeführt, nachdem IBM Spectrum Protect Plus den Datenträger aus dem vSnap-Repository bereitgestellt hat. Verwenden Sie die Daten für die angepasste Wiederherstellung aus den Dateien auf dem bereitgestellten Datenträger.
   - **Produktion**: In diesem Modus kopiert der Db2-Anwendungsserver zunächst die Dateien von dem vSnap-Repository-Datenträger auf den Zielhost, der entweder eine alternative Position oder die ursprüngliche Instanz ist. Diese kopierten Daten werden dann verwendet, um die Datenbank zu starten.
   - **Test**: In diesem Modus erstellt der Agent eine neue Datenbank, indem er die Datendateien direkt aus dem vSnap-Repository verwendet.
   - Fügen Sie einen Datenbanknamen hinzu, wenn die Datenbank an eine andere Position zurückgeschrieben wird und die Datenbank umbenannt werden soll.

   Tipp:

   "Produktion" ist die einzige verfügbare **Zurückschreibungsmethode** für Zurückschreibungsoperationen an die ursprüngliche Position. Alle Optionen, die für die von Ihnen ausgewählte Zurückschreibungsoperation nicht geeignet sind, sind nicht auswählbar.

   Um Daten in die ursprüngliche Instanz zurückzuschreiben, führen Sie die Anweisungen in In ursprüngliche Instanz zurückschreiben aus. Um Daten in eine alternative Instanz zurückzuschreiben, führen Sie die Anweisungen in In alternative Instanz zurückschreiben aus.

8. Legen Sie das Ziel für die Zurückschreibungsoperation fest, indem Sie eine der folgenden Optionen auswählen. Klicken Sie auf **Weiter**, um fortzufahren.

- **In ursprüngliche Instanz zurückschreiben**: Mit dieser Option werden Daten auf den ursprünglichen Server und in die ursprüngliche Instanz zurückgeschrieben.
- **In alternative Instanz zurückschreiben**: Mit dieser Option werden Daten an eine andere angegebene Position zurückgeschrieben, wobei eine Kopie der Daten an dieser Position erstellt wird.

Wenn die Zurückschreibung von Daten an eine alternative Position erfolgt, wählen Sie in der Tabelle **Instanz** eine Instanz aus, bevor Sie auf **Weiter** klicken. Die alternative Instanz muss sich auf einer anderen Maschine befinden; nicht geeignete Instanzen sind für die Auswahl nicht verfügbar. Für Mehrpartitionsdatenbanken muss die Zielinstanz über dieselbe Gruppe von Partitionen wie auf einer einzelnen Maschine verfügen.

9. Wählen Sie auf der Seite **Joboptionen** die Wiederherstellungs-, Anwendungs- und erweiterten Optionen für die Zurückschreibungsoperation aus, die Sie definieren.

   Tipp:

   Wiederherstellungsoptionen sind für Instant Access-Zurückschreibungsjobs nicht verfügbar.

   - **Keine Wiederherstellung**. Mit dieser Option wird jede aktualisierende Wiederherstellung nach der Zurückschreibungsoperation übersprungen. Die Datenbank verbleibt in einem Status `Aktualisierende Wiederherstellung anstehend`, bis Sie entscheiden, ob die aktualisierende Wiederherstellung manuell ausgeführt werden soll.
   - **Bis zum Ende der Sicherung wiederherstellen**. Mit dieser Option wird die ausgewählte Datenbank mit ihrem Status zum Zeitpunkt der Erstellung der Sicherung wiederhergestellt. Der Wiederherstellungsprozess verwendet die Protokolldateien, die in der Db2-Datenbanksicherung eingeschlossen sind.
   - **Bis zum Ende der verfügbaren Protokolle wiederherstellen**. Diese Option ist nur verfügbar, wenn die Protokolle in der Db2-Sicherungsjobdefinition gesichert werden. IBM Spectrum Protect Plus verwendet den neuesten Zurückschreibungspunkt. Ein temporärer Zurückschreibungspunkt für Protokollsicherungen wird automatisch erstellt, sodass die Db2-Datenbank bis zum Ende der Protokolle aktualisierend wiederhergestellt werden kann. Diese Wiederherstellungsoption ist nicht verfügbar, wenn Sie einen bestimmten Zurückschreibungspunkt aus der Liste ausgewählt hatten. Diese Option ist nur verfügbar, wenn Sie einen bedarfsgesteuerten Job für die Zurückschreibung nach Zeitpunkt ausführen, der die neueste Sicherung verwendet.
   - **Bis zu einem bestimmten Zeitpunkt wiederherstellen**. Diese Option schließt alle Sicherungsdaten bis zu einem bestimmten Zeitpunkt ein. Diese Option ist nur verfügbar, wenn Sie Protokollsicherungen in Ihrer Db2-Sicherungsjobdefinition aktiviert haben. Konfigurieren Sie eine Wiederherstellung nach Zeitpunkt anhand eines bestimmten Datums und einer bestimmten Uhrzeit, wie beispielsweise `1. Januar 2019 12:18:00`. IBM Spectrum Protect Plus sucht die Zurückschreibungspunkte unmittelbar vor und nach dem ausgewählten Zeitpunkt. Während des Wiederherstellungsprozesses werden der ältere Datensicherungsdatenträger und der neuere Protokollsicherungsdatenträger bereitgestellt. Wenn der Zeitpunkt nach der letzten Sicherung liegt, wird ein temporärer Zurückschreibungspunkt erstellt. Diese Wiederherstellungsoption ist nicht verfügbar, wenn Sie einen bestimmten Zurückschreibungspunkt aus der Liste ausgewählt hatten. Diese Option ist nur verfügbar, wenn Sie einen bedarfsgesteuerten Job für die Zurückschreibung nach Zeitpunkt ausführen, der die neueste Sicherung verwendet.

   Tipp: Um die optionalen Schritte im Zurückschreibungsassistenten zu überspringen, wählen Sie **Optionale Schritte überspringen** aus und klicken Sie auf **Weiter**.

10. Optional: Wählen Sie auf der Seite **Joboptionen** die Anwendungsoptionen für die Zurückschreibungsoperation aus, die Sie definieren.

    Tipp:

    Anwendungsoptionen sind für Instant Access-Zurückschreibungsjobs nicht verfügbar.

    - **Vorhandene Datenbanken überschreiben**. Wählen Sie diese Option aus, um vorhandene Datenbanken zu ersetzen, die während der Wiederherstellung anhand der Sicherungskopie dieselben Namen haben. Wird diese Option nicht ausgewählt, schlägt der Zurückschreibungsjob fehl, wenn Datenbanken mit demselben Namen während der Zurückschreibungsoperation gefunden werden.

Wenn Sie diese Option auswählen, stellen Sie sicher, dass das Db2-Protokollverzeichnis und das Db2-Spiegelprotokollverzeichnis keine Daten enthält.

Achtung: Stellen Sie sicher, dass keine anderen Datenbanken das lokale Datenbankverzeichnis als ursprüngliche Datenbank gemeinsam nutzen, da diese Daten überschrieben werden, wenn diese Option ausgewählt wird.

- **Maximale Anzahl paralleler Datenströme pro Datenbank**. Sie können auswählen, dass die Operation zum Zurückschreiben von Daten in parallelen Datenströmen ausgeführt werden soll. Diese Option ist nützlich, wenn eine große Datenbank zurückgeschrieben wird.
- **Größe der Db2-Datenbankspeichergruppe in KB angeben**. Geben Sie den Speicher in KB an, der für die Datenbankzurückschreibung auf der Zielmaschine zugeordnet werden soll. Dieser Wert wird verwendet, um die Größe des gemeinsam genutzten Speichers der Db2-Datenbank auf dem Zielserver zu ändern. Um dieselbe Größe des gemeinsam genutzten Speichers auf dem Quellenserver und dem Zielserver zu verwenden, setzen Sie den Wert auf Null.

11. Optional: Wählen Sie auf der Seite **Joboptionen** die erweiterten Optionen für die Zurückschreibungsoperation aus, die Sie definieren.
    - **Bereinigung direkt beim Fehlschlagen des Jobs ausführen**. Diese Option wird standardmäßig ausgewählt, um zugeordnete Ressourcen automatisch im Rahmen einer Zurückschreibungsoperation zu bereinigen, wenn die Wiederherstellung fehlschlägt.
    - **Mit Zurückschreibungen der anderen ausgewählten Datenbanken fortfahren, auch wenn eine Zurückschreibung fehlschlägt**. Mit dieser Option wird die Zurückschreibungsoperation fortgesetzt, wenn eine Datenbank in der Instanz nicht erfolgreich zurückgeschrieben werden kann. Der Prozess wird für alle anderen Datenbanken fortgesetzt, die zurückgeschrieben werden. Wird diese Option nicht ausgewählt, wird der Zurückschreibungsjob gestoppt, wenn die Wiederherstellung einer Ressource fehlschlägt.
    - **Protokollpriorität**: Wählen Sie bei einem **Instant Access**-Zurückschreibungsjob **iSCSI** oder **Fibre Channel** als Protokollpriorität aus, die für den Zurückschreibungsjob verwendet werden soll.
    - **Mountpunktpräfix**. Geben Sie für Instant Access-Zurückschreibungsoperationen das Präfix für den Pfad an, für den der Mountpunkt bereitgestellt werden soll.
12. Wählen Sie Scriptoptionen auf der Seite **Scripts anwenden** aus und klicken Sie auf **Weiter**, um fortzufahren.
    - Wählen Sie **Vorscript** aus, um ein hochgeladenes Script auszuwählen, und wählen Sie einen Anwendungs- oder Scriptserver aus, auf dem das Vorscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, auf dem das Script ausgeführt wird, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Rufen Sie die Seite **Systemkonfiguration** > **Script** auf, um Scripts und Scriptserver zu konfigurieren.
    - Wählen Sie **Nachscript** aus, um ein hochgeladenes Script auszuwählen, und wählen Sie einen Anwendungs- oder Scriptserver aus, auf dem das Nachscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, auf dem das Script ausgeführt wird, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Rufen Sie die Seite **Systemkonfiguration** > **Script** auf, um Scripts und Scriptserver zu konfigurieren.
    - Wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus, um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt. Wenn diese Option aktiviert ist und das Vorscript mit einem Rückkehrcode ungleich null beendet wird, wird die Ausführung des Sicherungs- oder Zurückschreibungsjobs fortgesetzt und der Taskstatus für das Vorscript gibt ABGESCHLOSSEN zurück. Wenn ein Nachscript mit einem Rückkehrcode ungleich null beendet wird, gibt der Taskstatus für das Nachscript ABGESCHLOSSEN zurück. Wenn diese Option nicht ausgewählt wird, wird der Sicherungs- oder Zurückschreibungsjob nicht ausgeführt und der Taskstatus für das Vorscript oder Nachscript gibt FEHLGESCHLAGEN zurück.
13. Ordnen Sie dem Zurückschreibungsjob auf der Seite **Zeitplan** einen Namen zu und wählen Sie die Ausführungshäufigkeit für den Job aus. Planen Sie die Startzeit und klicken Sie auf **Weiter**, um fortzufahren.

Wenn es sich bei dem Zurückschreibungsjob um einen bedarfsgesteuerten Job handelt, ist keine Option zur Eingabe eines Zeitplans vorhanden. Geben Sie einen Zeitplan nur für sich wiederholende Zurückschreibungsjobs an.

14. Überprüfen Sie auf der Seite **Überprüfen** Ihre Auswahlangaben für den Zurückschreibungsjob. Wenn alle Details für Ihren Zurückschreibungsjob korrekt sind, klicken Sie auf **Übergeben** oder klicken Sie auf **Zurück**, um Änderungen vorzunehmen.

Ergebnisse

Wenige Augenblicke nachdem Sie auf **Übergeben** geklickt haben, wird der Satz **Bedarfsgesteuerte Zurückschreibung** dem Fenster **Jobsitzungen** hinzugefügt. Um den Fortschritt der Zurückschreibungsoperation anzuzeigen, erweitern Sie den Job. Sie können die Protokolldatei auch herunterladen, indem Sie auf das Symbol für Herunterladen klicken. Alle aktiven Jobs sind auf der Seite **Jobs und Operationen** **Aktive Jobs** anzeigbar.

Um Daten in die ursprüngliche Instanz zurückzuschreiben, führen Sie die Anweisungen in In ursprüngliche Instanz zurückschreiben aus. Um Daten in eine alternative Instanz zurückzuschreiben, führen Sie die Anweisungen in In alternative Instanz zurückschreiben aus.

Db2-Daten in die ursprüngliche Instanz zurückschreiben

Sie können eine Datenbanksicherung in die ursprüngliche Instanz auf dem ursprünglichen Host zurückschreiben. Sie können die neueste Sicherung oder eine frühere Db2-Datenbanksicherungsversion zurückschreiben. Wenn Sie eine Datenbank in ihre ursprüngliche Instanz zurückschreiben, können Sie sie nicht umbenennen. Mit dieser Zurückschreibungsoption wird eine vollständige Produktionsdatenzurückschreibung ausgeführt, und die vorhandenen Daten werden an der Zielsite überschrieben, wenn die Option **Vorhandene Datenbanken überschreiben** ausgewählt wird.

Vorbereitende Schritte

Wenn Ihre Db2-Umgebung partitionierte Datenbanken umfasst, werden die Daten aller Partitionen während der regelmäßigen Sicherungsjobs gesichert. Alle Instanzen werden im Fenster "Sicherung" aufgelistet. Instanzen mit mehreren Partitionen werden mit Partitionsnummern und Hostnamen angezeigt.

Bevor Sie einen Zurückschreibungsjob für Db2 erstellen, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Mindestens ein Db2-Sicherungsjob ist definiert und wird erfolgreich ausgeführt. Anweisungen zum Definieren eines Sicherungsjobs finden Sie in „Db2-Daten sichern” auf Seite 151.
- IBM Spectrum Protect Plus-Rollen und -Ressourcengruppen sind dem Benutzer zugeordnet, der den Zurückschreibungsjob definiert. Weitere Informationen zum Zuordnen von Rollen finden Sie in Kapitel 13, „Benutzerzugriff verwalten”, auf Seite 311.
- Bei einer Zurückschreibung aus einem IBM Spectrum Protect-Archiv werden Dateien vom Band in einen Staging-Pool migriert, bevor der Job gestartet wird. Abhängig von der Größe der Zurückschreibung kann dieser Prozess mehrere Stunden dauern.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **Db2** und klicken Sie auf **Zurückschreibungsjob erstellen**.

   Der Assistent "Momentaufnahmezurückschreibung" wird geöffnet.
2. Optional: Wenn der Zurückschreibungsassistent über die Seite **Jobs und Operationen** gestartet wurde, wählen Sie Db2 als den Quellentyp aus und klicken Sie auf **Weiter**.

   Tipp: Um eine Zusammenfassung Ihrer Auswahlangaben im Zurückschreibungsassistenten zu erhalten, bewegen Sie den Cursor im Navigationsfenster des Assistenten auf das Informationssymbol.

3. Klicken Sie auf der Seite **Quellenauswahl** auf eine Db2-Instanz, um die Datenbanken in dieser Instanz anzuzeigen. Wählen Sie eine Datenbank aus, indem Sie auf das Plussymbol neben dem Datenbanknamen klicken. Klicken Sie auf **Weiter**, um fortzufahren.
4. Wählen Sie auf der Seite **Quellenmomentaufnahme** den Typ der erforderlichen Zurückschreibungsoperation aus.
   - **Bedarfsgesteuert: Momentaufnahme**: Erstellt eine einmalige Zurückschreibungsoperation aus einer Datenbankmomentaufnahme. Der Job wird nicht als sich wiederholender Job definiert.
   - **Bedarfsgesteuert: Zeitpunkt**: Erstellt eine einmalige Zurückschreibungsoperation aus einer Sicherung der Datenbank nach Zeitpunkt. Der Job wird nicht als sich wiederholender Job definiert.
   - **Wiederholt auftretend**: Erstellt einen sich wiederholenden Job, der gemäß einem Zeitplan ausgeführt wird und wiederholt ausgeführt wird.

   Tipp:

   Für **Bedarfsgesteuert: Momentaufnahme** können Sie "Keine Wiederherstellung" oder "Bis zum Ende der Sicherung wiederherstellen" auswählen. Für einen Zurückschreibungsjob des Typs **Bedarfsgesteuert: Zeitpunkt** können Sie "Bis zum Ende der verfügbaren Protokolle wiederherstellen" oder "Bis zu einem bestimmten Zeitpunkt wiederherstellen" auswählen.
5. Wählen Sie auf derselben Seite wie folgt einen **Typ der Zurückschreibungsposition** aus:

Position	Anweisungen
Site	Wählen Sie diese Option aus, um Daten von der primären oder sekundären Site zurückzuschreiben. "Site" ist die einzige Auswahl für bedarfsgesteuerte Zurückschreibungsjobs nach Zeitpunkt.
Cloudauslagerung	Wählen Sie diese Option aus, um Daten aus Cloudspeicher zurückzuschreiben. Geben Sie den Zurückschreibungspunkt an, der für die Momentaufnahme verwendet werden soll.
Repository-Auslagerung	Wählen Sie diese Option aus, um Daten aus einem vSnap-Repository zurückzuschreiben. Geben Sie den Zurückschreibungspunkt an, der für die Momentaufnahme verwendet werden soll.
Cloudarchivierung	Wählen Sie diese Option aus, um Daten zurückzuschreiben, die in der Cloud archiviert sind. Geben Sie den Zurückschreibungspunkt an, der für die Momentaufnahme verwendet werden soll.
Repository-Archivierung	Wählen Sie diese Option aus, um Daten zurückzuschreiben, die im vSnap-Repository archiviert sind. Geben Sie den Zurückschreibungspunkt an, der für die Momentaufnahme verwendet werden soll.

   Wenn Sie eine bedarfsgesteuerte Momentaufnahme erstellen, können Sie für die Momentaufnahme, nach der gesucht wird, einen Zeitraum angeben. Soweit zutreffend können Sie einen anderen vSnap-Server für die Operation verwenden.
6. Wählen Sie eine Position für die Zurückschreibungsoperation aus. Wählen Sie eine der folgenden Optionen für die Position aus und klicken Sie auf **Weiter**.

Option	Bezeichnung
Demo	Wählen Sie diese Option aus, um Daten vom vSnap-Demonstrationsserver zurückzuschreiben. Diese Option ist nur in bestimmten Konfigurationen verfügbar.

Option	Bezeichnung
Primär	Wählen Sie diese Option aus, um Daten aus dem primären vSnap-Server an das Ziel zurückzuschreiben. Diese Position ist für den Zurückschreibungspositionstyp Site verfügbar.
Sekundär	Wählen Sie diese Option aus, um Daten aus dem sekundären vSnap-Server an das Ziel zurückzuschreiben. Diese Position ist für den Zurückschreibungspositionstyp Site verfügbar.

Zurückschreibungspunkte sind über das Menü **Zurückschreibungspunkt** verfügbar.

7. Wählen Sie auf der Seite **Zurückschreibungsmethode** für die Zurückschreibungsoperation **Produktion** aus.

   Im Modus **Produktion** kopiert der Db2 zunächst die Dateien von dem vSnap-Repository-Datenträger auf den Zielhost. Diese kopierten Daten werden dann verwendet, um die Datenbank zu starten.

   Tipp: Geben Sie bei einer Zurückschreibungsoperation im Modus "Produktion" keinen neuen Datenbanknamen ein, da dieser nicht implementiert wird.
8. Legen Sie das Ziel für die Zurückschreibungsoperation mit **In ursprüngliche Instanz zurückschreiben** fest, um Daten auf den ursprünglichen Server zurückzuschreiben. Klicken Sie auf **Weiter**, um fortzufahren.
9. Wählen Sie wie in „Db2-Daten zurückschreiben” auf Seite 157 beschrieben Optionen aus.
10. Ordnen Sie dem Zurückschreibungsjob auf der Seite **Zeitplan** einen Namen zu und wählen Sie die Ausführungshäufigkeit für den Job aus. Planen Sie die Startzeit und klicken Sie auf **Weiter**, um fortzufahren.

    Wenn es sich bei dem Zurückschreibungsjob um einen bedarfsgesteuerten Job handelt, ist keine Option zur Eingabe eines Zeitplans vorhanden. Geben Sie einen Zeitplan nur für sich wiederholende Zurückschreibungsjobs an.
11. Überprüfen Sie auf der Seite **Überprüfen** Ihre Auswahlangaben für den Zurückschreibungsjob. Wenn alle Details für Ihren Zurückschreibungsjob korrekt sind, klicken Sie auf **Übergeben** oder klicken Sie auf **Zurück**, um Änderungen vorzunehmen.

Ergebnisse

Wenige Augenblicke nachdem Sie auf **Übergeben** geklickt haben, wird der Satz **Bedarfsgesteuerte Zurückschreibung** dem Fenster **Jobsitzungen** hinzugefügt. Um den Fortschritt der Zurückschreibungsoperation anzuzeigen, erweitern Sie den Job. Sie können die Protokolldatei auch herunterladen, indem Sie auf das Symbol für Herunterladen klicken. Alle aktiven Jobs sind auf der Seite **Jobs und Operationen** **Aktive Jobs** anzeigbar.

Db2-Datenbanken in eine alternative Instanz zurückschreiben

Sie können eine Db2-Datenbank in eine andere Db2-Instanz auf einem alternativen Host zurückschreiben. Sie können eine Datenbank auch in eine Instanz mit einem anderen Namen zurückschreiben und die Datenbank umbenennen. Bei diesem Prozess wird eine exakte Kopie der Datenbank auf einem anderen Host in einer anderen Instanz erstellt. Wenn Sie eine Ressource in eine alternative Position zurückschreiben, können Sie dieselbe Ressource mehrmals ohne Angabe anderer Zielhosts zurückschreiben.

Vorbereitende Schritte

Wichtig: Für alle Zurückschreibungsoperationen muss Db2 auf den Quellen- und Zielhosts denselben Versionsstand haben. Zusätzlich zu dieser Anforderung müssen Sie sicherstellen, dass auf jedem Host eine Instanz vorhanden ist, die denselben Namen wie die Instanz hat, die zurückgeschrieben wird. Diese Anforderung gilt, wenn die Zielinstanz denselben Namen hat und wenn die Namen unterschiedlich sind.

Damit die Zurückschreibungsoperation erfolgreich ausgeführt werden kann, müssen beide Instanzen bereitgestellt werden, eine mit dem ursprünglichen Namen und die andere mit dem neuen Namen.

Bevor Sie einen Zurückschreibungsjob für Db2 erstellen, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Mindestens ein Db2-Sicherungsjob ist definiert und wird erfolgreich ausgeführt. Anweisungen zum Definieren eines Sicherungsjobs finden Sie in „Db2-Daten sichern" auf Seite 151.
- IBM Spectrum Protect Plus-Rollen und -Ressourcengruppen sind dem Benutzer zugeordnet, der den Zurückschreibungsjob definiert. Weitere Informationen zum Zuordnen von Rollen finden Sie in Kapitel 13, „Benutzerzugriff verwalten", auf Seite 311.
- Bei einer Zurückschreibung aus einem IBM Spectrum Protect-Archiv werden Dateien vom Band in einen Staging-Pool migriert, bevor der Job gestartet wird. Abhängig von der Größe der Zurückschreibung kann dieser Prozess mehrere Stunden dauern.

Bevor Sie eine Operation zum Zurückschreiben in eine alternative Instanz starten, stellen Sie sicher, dass die Dateisystemstruktur auf der Quellenmaschine mit der auf der Zielmaschine übereinstimmt. Diese Dateisystemstruktur umfasst Tabellenbereiche, Onlineprotokolle und das lokale Datenbankverzeichnis. Stellen Sie sicher, dass dedizierte Datenträger mit genügend Speicherbereich der Dateisystemstruktur zugeordnet werden. Db2 muss für alle Zurückschreibungsoperationen über denselben Versionsstand auf dem Quellen- und dem Zielhost verfügen und eine Instanz mit demselben Namen muss auf jedem Host vorhanden sein. Weitere Informationen zu den Speicheranforderungen finden Sie in Speicheranforderungen für Db2-Schutz. Weitere Informationen zu den Voraussetzungen und zur Konfiguration finden Sie in Voraussetzungen für Db2.

Einschränkung: Wenn Daten in dem lokalen Datenbankverzeichnis vorhanden sind, in das die Datenbanksicherung zurückgeschrieben wird, und die Option **Vorhandene Datenbanken überschreiben** nicht ausgewählt wird, schlägt die Zurückschreibungsoperation fehl. Keine anderen Daten können das lokale Datenbankverzeichnis gemeinsam nutzen, in das die Sicherung zurückgeschrieben wird. Wenn die Option **Vorhandene Datenbanken überschreiben** ausgewählt wird, werden alle vorhandenen Daten aus dem lokalen Datenbankverzeichnis auf dem alternativen Host entfernt.

Anmerkung: Wenn Sie Datenbanken mit mehreren Partitionen an eine alternative Position zurückschreiben, stellen Sie sicher, dass die Zielinstanz mit denselben Partitionsnummern wie die ursprüngliche Instanz konfiguriert ist. Alle diese Partitionen müssen sich auf einem einzigen Host befinden. Wenn Daten in eine neue Instanz zurückgeschrieben werden, die umbenannt wird, müssen beide Instanzen, die für die Zurückschreibungsoperation erforderlich sind, mit derselben Anzahl Partitionen konfiguriert werden.

Informationen zu diesem Vorgang

Stellen Sie sicher, dass die Plattenpfade für die umgeleitete Zurückschreibungsoperation den Instanznamen und den Datenbanknamen einschließen. Die Informationen werden für alle Typen von Pfaden benötigt: Datenbankpfade, Containerpfade, Speicherpfade sowie Protokoll- und Spiegelprotokollpfade.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **Db2** und klicken Sie auf **Zurückschreibungsjob erstellen**.

   Der Assistent "Momentaufnahmezurückschreibung" wird geöffnet.
2. Optional: Wenn der Zurückschreibungsassistent über die Seite **Jobs und Operationen** gestartet wurde, wählen Sie Db2 als den Quellentyp aus und klicken Sie auf **Weiter**.

   Tipp: Um eine Zusammenfassung Ihrer Auswahlangaben im Zurückschreibungsassistenten zu erhalten, bewegen Sie den Cursor im Navigationsfenster des Assistenten auf das Informationssymbol.
3. Klicken Sie auf der Seite **Quellenauswahl** auf eine Db2-Instanz, um die Datenbanken in dieser Instanz anzuzeigen. Wählen Sie eine Datenbank aus, indem Sie auf das Plussymbol neben dem Datenbanknamen klicken. Klicken Sie auf **Weiter**, um fortzufahren.
4. Wählen Sie auf der Seite **Quellenmomentaufnahme** den Typ der erforderlichen Zurückschreibungsoperation aus.

- **Bedarfsgesteuert: Momentaufnahme**: Erstellt eine einmalige Zurückschreibungsoperation aus einer Datenbankmomentaufnahme. Der Job wird nicht als sich wiederholender Job definiert.
- **Bedarfsgesteuert: Zeitpunkt**: Erstellt eine einmalige Zurückschreibungsoperation aus einer Sicherung der Datenbank nach Zeitpunkt. Der Job wird nicht als sich wiederholender Job definiert.
- **Wiederholt auftretend**: Erstellt einen sich wiederholenden Job, der gemäß einem Zeitplan ausgeführt wird und wiederholt ausgeführt wird.

Tipp:

Für **Bedarfsgesteuert: Momentaufnahme** können Sie "Keine Wiederherstellung" oder "Bis zum Ende der Sicherung wiederherstellen" auswählen. Für einen Zurückschreibungsjob des Typs **Bedarfsgesteuert: Zeitpunkt** können Sie "Bis zum Ende der verfügbaren Protokolle wiederherstellen" oder "Bis zu einem bestimmten Zeitpunkt wiederherstellen" auswählen.

5. Wählen Sie auf derselben Seite wie folgt einen **Typ der Zurückschreibungsposition** aus:

Position	Anweisungen
Site	Wählen Sie diese Option aus, um Daten von der primären oder sekundären Site zurückzuschreiben. "Site" ist die einzige Auswahl für bedarfsgesteuerte Zurückschreibungsjobs nach Zeitpunkt.
Cloudauslagerung	Wählen Sie diese Option aus, um Daten aus Cloudspeicher zurückzuschreiben. Geben Sie den Zurückschreibungspunkt an, der für die Momentaufnahme verwendet werden soll.
Repository-Auslagerung	Wählen Sie diese Option aus, um Daten aus einem vSnap-Repository zurückzuschreiben. Geben Sie den Zurückschreibungspunkt an, der für die Momentaufnahme verwendet werden soll.
Cloudarchivierung	Wählen Sie diese Option aus, um Daten zurückzuschreiben, die in der Cloud archiviert sind. Geben Sie den Zurückschreibungspunkt an, der für die Momentaufnahme verwendet werden soll.
Repository-Archivierung	Wählen Sie diese Option aus, um Daten zurückzuschreiben, die im vSnap-Repository archiviert sind. Geben Sie den Zurückschreibungspunkt an, der für die Momentaufnahme verwendet werden soll.

Wenn Sie eine bedarfsgesteuerte Momentaufnahme erstellen, können Sie für die Momentaufnahme, nach der gesucht wird, einen Zeitraum angeben. Soweit zutreffend können Sie einen anderen vSnap-Server für die Operation verwenden.

6. Wählen Sie eine Position für die Zurückschreibungsoperation aus. Wählen Sie eine der folgenden Optionen für die Position aus und klicken Sie auf **Weiter**.

Option	Bezeichnung
Demo	Wählen Sie diese Option aus, um Daten vom vSnap-Demonstrationsserver zurückzuschreiben. Diese Option ist nur in bestimmten Konfigurationen verfügbar.
Primär	Wählen Sie diese Option aus, um Daten aus dem primären vSnap-Server an das Ziel zurückzuschreiben. Diese Position ist für den Zurückschreibungspositionstyp Site verfügbar.

Option	Bezeichnung
Sekundär	Wählen Sie diese Option aus, um Daten aus dem sekundären vSnap-Server an das Ziel zurückzuschreiben. Diese Position ist für den Zurückschreibungspositionstyp Site verfügbar.

Zurückschreibungspunkte sind über das Menü **Zurückschreibungspunkt** verfügbar.

7. Wählen Sie eine für das für die Zurückschreibungsoperation ausgewählte Ziel geeignete **Zurückschreibungsmethode** aus. Klicken Sie auf **Weiter**, um fortzufahren.
   - **Produktion**: In diesem Modus kopiert der Db2-Anwendungsserver zunächst die Dateien von dem vSnap-Repository-Datenträger auf den Zielhost, der entweder eine alternative Position oder die ursprüngliche Instanz ist. Diese kopierten Daten werden dann verwendet, um die Datenbank zu starten.
   - **Test**: In diesem Modus erstellt der Agent eine neue Datenbank, indem er die Datendateien direkt aus dem vSnap-Repository verwendet.
   - **Instant Access**: In diesem Modus wird keine weitere Aktion ausgeführt, nachdem IBM Spectrum Protect Plus den Datenträger aus dem vSnap-Repository bereitgestellt hat. Verwenden Sie die Daten für die angepasste Wiederherstellung aus den Dateien auf dem bereitgestellten Datenträger.
   - Fügen Sie einen Datenbanknamen hinzu, wenn die Datenbank an eine andere Position zurückgeschrieben wird und die Datenbank umbenannt werden soll.
8. Legen Sie das Ziel für die Zurückschreibungsoperation mit **In alternative Instanz zurückschreiben** fest, um Daten an eine andere Position zurückzuschreiben, die Sie aus der Liste auswählbarer Positionen auswählen können. Klicken Sie auf **Weiter**, um fortzufahren.

   Wenn die Zurückschreibung an eine alternative Position erfolgt, wählen Sie in der Tabelle **Instanz** eine Instanz aus, bevor Sie auf **Weiter** klicken. Zielinstanzen, die nicht geeignet sind, können nicht ausgewählt werden.
9. Wählen Sie wie in „Db2-Daten zurückschreiben” auf Seite 157 beschrieben Optionen aus.
10. Ordnen Sie dem Zurückschreibungsjob auf der Seite **Zeitplan** einen Namen zu und wählen Sie die Ausführungshäufigkeit für den Job aus. Planen Sie die Startzeit und klicken Sie auf **Weiter**, um fortzufahren.

    Wenn es sich bei dem Zurückschreibungsjob um einen bedarfsgesteuerten Job handelt, ist keine Option zur Eingabe eines Zeitplans vorhanden. Geben Sie einen Zeitplan nur für sich wiederholende Zurückschreibungsjobs an.
11. Überprüfen Sie auf der Seite **Überprüfen** Ihre Auswahlangaben für den Zurückschreibungsjob. Wenn alle Details für Ihren Zurückschreibungsjob korrekt sind, klicken Sie auf **Übergeben** oder klicken Sie auf **Zurück**, um Änderungen vorzunehmen.

Ergebnisse

Wenige Augenblicke nachdem Sie auf **Übergeben** geklickt haben, wird der Satz **Bedarfsgesteuerte Zurückschreibung** dem Fenster **Jobsitzungen** hinzugefügt. Um den Fortschritt der Zurückschreibungsoperation anzuzeigen, erweitern Sie den Job. Sie können die Protokolldatei auch herunterladen, indem Sie auf das Symbol für Herunterladen klicken. Alle aktiven Jobs sind auf der Seite **Jobs und Operationen** **Aktive Jobs** anzeigbar.

Microsoft Exchange Server

Nachdem Sie einen Microsoft Exchange Server erfolgreich registriert haben, ist der Schutz von Microsoft Exchange-Daten mit IBM Spectrum Protect Plus möglich. Definieren Sie eine SLA-Richtlinie (SLA = Service-Level-Agreement), um Sicherungsjobs mit bestimmten Zeitplänen, Aufbewahrungsrichtlinien und Scripts zu erstellen.

Voraussetzungen für Microsoft Exchange Server

Stellen Sie sicher, dass alle Voraussetzungen für Ihre Microsoft Exchange-Anwendung erfüllt sind, bevor Sie Microsoft Exchange-Datenbanken mit IBM Spectrum Protect Plus schützen.

Weitere Informationen finden Sie in „Microsoft Exchange Server-Anforderungen” auf Seite 28.

Virtualisierungsunterstützung

IBM Spectrum Protect Plus unterstützt die Ausführung von Microsoft Exchange Server sowohl auf einem physischen Server (Bare-Metal-Server) als auch in einer Virtualisierungsumgebung. Die folgenden Virtualisierungsumgebungen werden unterstützt:

- VMware ESX-Gastbetriebssystem
- Microsoft Windows-Hyper-V-Gastbetriebssystem

Berechtigungen

Um sicherzustellen, dass ein Microsoft Exchange-Agent in Ihrer IBM Spectrum Protect Plus-Umgebung funktionsfähig ist, müssen Sie entsprechende Berechtigungen definieren.

Rollenbasierte Zugriffssteuerung

Aus Sicherheitsgründen müssen bei IBM Spectrum Protect Plus Benutzer, die bei dem Exchange-Server angemeldet sind, RBAC-Berechtigungen (RBAC = rollenbasierte Zugriffssteuerung) verfügen, um auf Mailboxen zugreifen und Mailboxzurückschreibungstasks ausführen zu können.

Sie müssen jedem Exchange-Benutzer, der Mailboxzurückschreibungstasks ausführen wird, die folgenden Verwaltungsrollen zuordnen:

- Active Directory-Berechtigungen
- ApplicationImpersonation
- Datenbanken
- Notfallwiederherstellung
- Postfachimport/-export
- Öffentliche Ordner
- Konfiguration (nur Anzeige)
- Empfänger (nur Anzeige)

Es wird empfohlen, Benutzer, die Mailboxzurückschreibungstasks ausführen sollen, einer Exchange Server-Rollengruppe hinzuzufügen, die die oben genannten Rollen enthält.

Exchange Server umfasst eine Reihe von integrierten Rollengruppen. Die Rollengruppe "Organisationsverwaltung" enthält standardmäßig die meisten, wenn nicht sogar alle, der oben aufgelisteten Rollen.

Es wird empfohlen, die Benutzer, die Mailboxzurückschreibungstasks ausführen sollen, der Rollengruppe "Organisationsverwaltung" hinzuzufügen und sicherzustellen, dass diese Gruppe alle der oben aufgelisteten Rollen enthält.

Es ist auch möglich, die Benutzer einer anderen von Ihnen erstellten Rollengruppe oder jeder anderen integrierten Rollengruppe hinzuzufügen, die die oben aufgelisteten Rollen enthält.

Anmerkung: Bei einem Benutzer, dessen Name in der Exchange-Rollengruppe "Organisationsverwaltung" oder deren Untergruppen nicht vorhanden ist, kann die Ausführung von Mailboxzurückschreibungsoperationen langsamer erfolgen.

Anmerkung: Sie können Exchange-Rollengruppen **nur** dann mithilfe der Exchange Admin Center-(EAC-) oder Exchange Powershell-Cmdlets verwalten, wenn Ihr Benutzername durch die Sicherheitsrichtlinie in Ihrer Organisation dazu berechtigt ist.

Geltungsbereich für Verwaltungsrollen

Stellen Sie sicher, dass sich die folgenden Exchange-Objekte im Geltungsbereich für Verwaltungsrollen des Exchange-Benutzers befinden:

- Der Exchange-Server, der die erforderlichen Daten enthält
- Die von IBM Spectrum Protect Plus erstellte Wiederherstellungsdatenbank
- Die Datenbank, die die aktive Mailbox enthält
- Die Datenbank, die die aktive Mailbox des Benutzers enthält, der die Zurückschreibungsoperation ausführt

Stellen Sie sicher, dass der Exchange-Benutzername zur lokalen Gruppe "Administratoren" gehört und in der Domäne über eine aktive Exchange-Mailbox verfügt. Windows fügt die Gruppe "Exchange-Organisationsadministratoren" standardmäßig anderen Sicherheitsgruppen hinzu, einschließlich der lokalen Gruppe "Administratoren". Für Exchange-Benutzer, die nicht zur Exchange-Gruppe "Organisationsverwaltung" gehören, müssen Sie den Benutzeraccount der lokalen Gruppe "Administratoren" manuell mithilfe des Tools "Lokale Benutzer und Gruppen" auf dem Computer des Domänenmitglieds hinzufügen.

Klicken Sie auf dem Computer des Domänenmitglieds auf **Verwaltung > Computerverwaltung > Lokale Benutzer und Gruppen**. Fügen Sie auf einem Domänen-Controller-Computer, auf dem keine lokale Gruppe "Administratoren" bzw. kein Tool "Lokale Benutzer und Gruppen" verfügbar ist, den Benutzeraccount manuell der Gruppe "Administratoren" in der Domäne hinzu, indem Sie auf **Verwaltung > Active Directory-Benutzer und -Gruppen** klicken.

Encrypted File System

IBM Spectrum Protect Plus für Exchange erfordert, dass das Encrypted File System (EFS) in der lokalen oder Gruppendomänenrichtlinie aktiviert ist und ein gültiges DRA-Zertifikat für die Domäne verfügbar ist. Wenn eine angepasste Gruppenrichtlinie definiert und mit der Organisationseinheit verknüpft ist, stellen Sie sicher, dass der Exchange-Server zu der Organisationseinheit gehört.

Microsoft Exchange-Anwendungsserver hinzufügen

Wenn Sie Microsoft Exchange Server registrieren, wird IBM Spectrum Protect Plus ein Bestand von Exchange-Datenbanken hinzugefügt. Ist der Bestand verfügbar, können Sie mit der Sicherung und Zurückschreibung Ihrer Exchange-Datenbanken beginnen und Berichte erstellen.

Informationen zu diesem Vorgang

Um einen Microsoft Exchange-Anwendungsserver zu registrieren, benötigen Sie die IP-Adresse oder den Hostnamen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Microsoft Exchange-Anwendungsserver hinzuzufügen:

1. Erweitern Sie im Navigationsfenster **Schutz verwalten > Anwendungen > Exchange**.
2. Klicken Sie auf der Seite **Exchange** auf **Anwendungsserver verwalten** und klicken Sie dann auf **Anwendungsserver hinzufügen**, um das Hostsystem hinzuzufügen.
3. Geben Sie in der Maske **Anwendungseigenschaften** die IP- oder Hostadresse ein.
4. Geben Sie eine Benutzer-ID im Format mit Active Directory-Domäne und Benutzeraccount (Domäne \Benutzer) sowie das zugeordnete Kennwort ein. Dieser Benutzer muss über die korrekten Exchange-Rollen und -Berechtigungen verfügen. Weitere Informationen zu Exchange-Berechtigungen finden Sie in „Berechtigungen” auf Seite 168.
5. Klicken Sie auf **Speichern** und wiederholen Sie die Schritte, um IBM Spectrum Protect Plus andere Microsoft Exchange-Instanzen hinzuzufügen.

   Wichtig: Registrieren Sie in einer Umgebung mit Datenbankverfügbarkeitsgruppen (Database Availability Group = DAG) alle Microsoft Exchange-Anwendungsserver in der DAG.

Nächste Schritte

Wenn Sie IBM Spectrum Protect Plus Ihre Exchange-Anwendungsserver hinzufügen, wird automatisch auf jeder Instanz eine Bestandsverarbeitung ausgeführt. Datenbanken müssen erkannt werden, damit sie gesichert werden können. Sie können zu jeder Zeit eine manuelle Bestandsverarbeitung ausführen, um Aktualisierungen zu erkennen. Anweisungen zur Ausführung einer manuellen Bestandsverarbeitung finden Sie in „Microsoft Exchange-Datenbanken durch eine Bestandsverarbeitung erkennen" auf Seite 170. Anweisungen zum Definieren von Exchange-Datenbanksicherungsjobs finden Sie in „SLA-Sicherungsjob definieren" auf Seite 171.

Microsoft Exchange-Datenbanken durch eine Bestandsverarbeitung erkennen

Wenn Sie IBM Spectrum Protect Plus Ihre Microsoft Exchange Server-Instanzen hinzufügen, wird automatisch eine Bestandsverarbeitung ausgeführt. Sie können jedoch zu jeder Zeit manuell eine Bestandsverarbeitung auf einem Exchange-Anwendungsserver ausführen, um Aktualisierungen zu erkennen und alle Exchange-Datenbanken für jede Instanz aufzulisten.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie IBM Spectrum Protect Plus Ihre Exchange-Instanzen hinzugefügt haben. Anweisungen zum Hinzufügen einer Exchange-Instanz finden Sie in „Microsoft Exchange-Anwendungsserver hinzufügen" auf Seite 169.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **Exchange**.
2. Klicken Sie auf **Bestandsverarbeitung ausführen**.

   Bei der Ausführung der Bestandsverarbeitung ändert sich die Schaltflächenbeschriftung in **Bestandsverarbeitung wird ausgeführt**. Sie können eine Bestandsverarbeitung auf jedem verfügbaren Anwendungsserver ausführen, Sie können jedoch nur jeweils einen einzigen Bestandsprozess ausführen.
3. Um den Bestandsjob zu überwachen, rufen Sie **Jobs und Operationen** auf. Klicken Sie auf die Registerkarte **Aktive Jobs** und suchen Sie nach dem neuesten Bestandsprotokolleintrag für den Anwendungsserver.

   Beendete Jobs werden auf der Registerkarte **Jobprotokoll** angezeigt. Mithilfe der Liste **Sortieren nach** können Sie Jobs auf der Basis von Startzeit, Typ, Status, Jobnamen oder Dauer sortieren. Verwenden Sie das Feld **Nach Namen suchen**, um nach Jobs anhand des Namens zu suchen. Sie können Sterne als Platzhalterzeichen in dem Namen verwenden.
4. Wenn der Bestandsjob abgeschlossen ist, klicken Sie im Fenster **Exchange-Sicherung** auf eine Exchange-Instanz, um eine Sicht zu öffnen, in der die für diese Instanz erkannten Datenbanken angezeigt werden. Wenn Datenbanken in der Liste **Instanzen** fehlen, überprüfen Sie Ihren Microsoft Exchange-Anwendungsserver und führen Sie den Bestandsjob erneut aus.

   Tipp: Um zur Liste der Instanzen zurückzukehren, klicken Sie auf den Hypertext **Instanzen** im Fenster "Exchange-Sicherung".

Microsoft Exchange-Verbindung testen

Nachdem Sie einen Microsoft Exchange-Anwendungsserver registriert und ihn zur Anwendungsserverliste hinzugefügt haben, testen Sie die Verbindung. Bei dem Test wird die Kommunikation zwischen IBM Spectrum Protect Plus und dem Hostanwendungsserver verifiziert.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **Exchange**.
2. Klicken Sie auf der Seite **Exchange** auf **Anwendungsserver verwalten**.

   Die verfügbaren Microsoft Exchange-Anwendungsserver werden angezeigt.
3. Klicken Sie für den Microsoft Exchange-Anwendungsserver, der getestet werden soll, auf **Aktionen** und klicken Sie dann auf **Testen**.

Der Testbericht zeigt eine Liste der ausgeführten Tests und ihren Status. Jede Testprozedur umfasst einen Test der Netzkonfiguration des physischen Hosts, einen Test der fernen Sitzung und einen Test der Windows-Voraussetzungen wie z. B. Benutzeradministratorberechtigungen.

4. Klicken Sie auf **OK**, um den Test abzuschließen. Führen Sie den Test erneut aus, nachdem Sie alle Probleme behoben haben.

Microsoft Exchange-Datenbanken sichern

Um Microsoft Exchange-Datenbanken zu schützen, können Sie einen Sicherungsjob definieren, der kontinuierlich ausgeführt wird, um Teilsicherungen zu erstellen. Sie können auch bedarfsgesteuerte Sicherungsjobs außerhalb des Zeitplans ausführen.

Vorbereitende Schritte

Stellen Sie sicher, dass die Anwendungsserver, die die zu sichernden Exchange-Datenbanken enthalten, hinzugefügt werden. Weitere Informationen finden Sie in „Microsoft Exchange-Anwendungsserver hinzufügen” auf Seite 169.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **Exchange**.
2. Klicken Sie im Fenster **Exchange-Sicherung** auf die Microsoft Exchange-Instanz und wählen Sie dann die Datenbank aus, die gesichert werden soll.

   Jede Datenbank wird nach dem Instanz- oder Datenbanknamen, der angewendeten SLA-Richtlinie und der Wählbarkeit für die Protokollsicherung aufgelistet.
3. Klicken Sie auf **Ausführen**.

   Der Sicherungsjob startet und Sie können die Details über **Jobs und Operationen** > **Aktive Jobs** anzeigen.

   Tipp: Die Schaltfläche **Ausführen** ist nur für die Sicherung einer einzelnen Datenbank aktiviert; auf die Datenbank muss außerdem eine SLA-Richtlinie angewendet sein.
4. Um Sicherungsjobs für mehrere Datenbanken auszuführen, wählen Sie die Datenbanken im Fenster "Exchange-Sicherung" aus und klicken Sie auf **SLA-Richtlinie auswählen**.

   Weitere Informationen zum Definieren von Sicherungsjobs mit SLA-Richtlinien und zum Definieren von Optionen für Sicherungsjobs finden Sie in „SLA-Sicherungsjob definieren” auf Seite 171.

SLA-Sicherungsjob definieren

Wenn Ihre Microsoft Exchange-Datenbanken für alle Ihre Exchange-Instanzen aufgelistet werden, wählen Sie eine SLA-Richtlinie (SLA = Service-Level-Agreement) aus und wenden Sie die Richtlinie an, um Ihre Daten zu schützen.

Informationen zu diesem Vorgang

IBM Spectrum Protect Plus unterstützt eine oder mehrere Microsoft Exchange-Datenbanken pro Exchange-Sicherungsjob. Mehrere Datenbanksicherungsjobs werden sequenziell ausgeführt.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **Exchange**.
2. Wählen Sie eine Exchange-Instanz aus, um alle Daten in dieser Instanz zu sichern, oder klicken Sie auf einen Instanznamen und wählen Sie dann einzelne Datenbanken aus, die gesichert werden sollen.
3. Klicken Sie auf **SLA-Richtlinie auswählen** und wählen Sie eine SLA-Richtlinie aus.

   Die vordefinierten Auswahlmöglichkeiten sind "Gold", "Silber" und "Bronze". Sie verfügen über verschiedene Häufigkeiten und Aufbewahrungsraten. Gold ist die häufigste mit der geringsten Aufbewahrungsrate. Sie können auch eine angepasste SLA-Richtlinie erstellen oder eine vorhandene Richtlinie editieren. Weitere Informationen finden Sie in „SLA-Richtlinie erstellen” auf Seite 93.
4. Klicken Sie auf **Optionen auswählen**, um Optionen für Ihre Sicherung zu definieren, wie z. B. Aktivierung von Protokollsicherungen für zukünftige Wiederherstellungsoptionen und Angabe der Anzahl pa-

ralleler Datenströme, um den Zeitaufwand für die Sicherung großer Datenbanken zu reduzieren. Speichern Sie Ihre Änderungen.

5. Konfigurieren Sie die SLA-Richtlinie, indem Sie auf das Symbol in der Spalte **Richtlinienoptionen** der Tabelle **SLA-Richtlinienstatus** klicken.

   Weitere Informationen zu SLA-Konfigurationsoptionen finden Sie in „SLA-Konfigurationsoptionen für einen Sicherungsjob definieren" auf Seite 172.

6. Soll die Richtlinie außerhalb des geplanten Jobs ausgeführt werden, wählen Sie die Instanz oder Datenbank aus und klicken Sie dann auf **Aktionen** > **Starten**.

   Der Status ändert sich in **Aktiv** für die ausgewählte SLA-Richtlinie. Um den Zeitplan anzuhalten, klicken Sie auf **Aktionen** > **Zeitplan anhalten**. Um einen Job nach seinem Start abzubrechen, klicken Sie auf **Aktionen** > **Abbrechen**.

SLA-Konfigurationsoptionen für einen Sicherungsjob definieren

Nachdem Sie ein Service-Level-Agreement (SLA) für Ihren Sicherungsjob definiert haben, können Sie weitere Optionen für diesen Job konfigurieren. Zu den zusätzlichen SLA-Optionen gehören die Ausführung von Scripts, der Ausschluss von Ressourcen aus der Sicherungsoperation und das Erzwingen einer vollständigen Basissicherungskopie, sofern erforderlich.

Vorgehensweise

1. Klicken Sie in der Spalte **Richtlinienoptionen** der Tabelle **SLA-Richtlinienstatus** für den Job, den Sie konfigurieren, auf das Zwischenablagesymbol, um zusätzliche Konfigurationsoptionen anzugeben.
2. Um eine Vorscriptkonfiguration zu definieren, wählen Sie **Vorscript** aus und führen Sie eine der folgenden Aktionen aus:
   - Um einen Scriptserver zu verwenden, wählen Sie **Scriptserver verwenden** aus und wählen Sie ein hochgeladenes Script aus der Liste **Script** oder **Scriptserver** aus.
   - Um ein Script auf einem Anwendungsserver auszuführen, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab und wählen Sie einen Anwendungsserver aus der Liste **Anwendungsserver** aus.
3. Um eine Nachscriptkonfiguration zu definieren, wählen Sie **Nachscript** aus und führen Sie eine der folgenden Aktionen aus:
   - Um einen Scriptserver zu verwenden, wählen Sie **Scriptserver verwenden** aus und wählen Sie ein hochgeladenes Script aus der Liste **Script** oder **Scriptserver** aus.
   - Um ein Script auf einem Anwendungsserver auszuführen, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab und wählen Sie einen Anwendungsserver aus der Liste **Anwendungsserver** aus.

   Scripts und Scriptserver werden auf der Seite **Systemkonfiguration** > **Script** konfiguriert. Weitere Informationen zum Arbeiten mit Scripts finden Sie in Scripts konfigurieren.
4. Wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus, um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt.

   Wenn diese Option ausgewählt wird und das Script die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird versucht, die Sicherungs- oder Zurückschreibungsoperation auszuführen, und der Taskstatus des Scripts wird als ABGESCHLOSSEN zurückgemeldet. Wenn diese Option nicht ausgewählt wird, wird nicht versucht, die Sicherung oder Zurückschreibung auszuführen, und der Taskstatus des Scripts wird als FEHLGESCHLAGEN zurückgemeldet.
5. Geben Sie Ressourcen an, um sie aus dem Sicherungsjob auszuschließen. Geben Sie einen genauen Ressourcennamen in das Feld **Ressourcen ausschließen** ein. Wenn Sie sich bezüglich eines Namens nicht sicher sind, verwenden Sie Sterne als Platzhalterzeichen, die vor dem Muster (**text*) oder hinter dem Muster (*text**) angegeben werden. Mehrere Platzhalterzeichen können mit alphanumerischen Standardzeichen und den folgenden Sonderzeichen eingegeben werden: - _ und *. Trennen Sie Einträge durch ein Semikolon voneinander.

6. Soll eine Gesamtsicherung einer bestimmten Ressource erstellt werden, geben Sie den Namen dieser Ressource in das Feld **Gesamtsicherung der Ressourcen erzwingen** ein. Trennen Sie mehrere Ressourcen durch ein Semikolon voneinander.

   Bei einer Gesamtsicherung wird einmalig die vorhandene Sicherung dieser Ressource ersetzt. Danach wird die Ressource wie zuvor mit Teilsicherungen gesichert.
7. Klicken Sie auf **Speichern**.

Microsoft Exchange-Datenbankprotokolle sichern
Sie können die Datenbanktransaktionsprotokolle für Microsoft Exchange-Datenbanken sichern. Exchange-Protokollsicherungen werden mithilfe des Windows-Taskplaners geplant. Wenn Protokollsicherungen verfügbar sind, können Sie eine aktualisierende Datenwiederherstellung während einer Zurückschreibungsoperation ausführen, um sicherzustellen, dass die Daten bis zum letzten möglichen Zeitpunkt wiederhergestellt werden.

Informationen zu diesem Vorgang

Wenn Protokollsicherungen aktiviert sind, wird eine Taskplaner-Task auf dem Exchange-Server erstellt. Die Task führt eine Sicherungsoperation für Ihre Exchange-Protokolldateien gemäß der SLA-Richtlinie aus.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **Exchange**.
2. Klicken Sie auf die Microsoft Exchange-Instanz, die geschützt werden soll, und wählen Sie dann die Datenbanken aus, deren Protokolle gesichert werden sollen.

   Tipp: Die Spalte **Für Protokollsicherung auswählbar** zeigt die Datenbanken an, für die Protokollsicherungen ausgeführt werden können. Wenn eine Datenbank als nicht auswählbar für die Protokollsicherung registriert ist, wird eine Erläuterung in der Kurzinfo bereitgestellt.
3. Klicken Sie auf **Optionen auswählen** und wählen Sie dann **Protokollsicherung aktivieren** aus.
4. Geben Sie die Häufigkeit der Protokollsicherungen in Tage, Stunden oder Minuten ein.
5. Wählen Sie das Startdatum und die Startzeit für die Protokollsicherungen aus und klicken Sie dann auf **Speichern**.

Ergebnisse
Die Datenbanktransaktionsprotokolle werden gemäß der ausgewählten Häufigkeit auf dem vSnap-Server gesichert.

Einschränkung: Die Datenbankprotokolle werden nur auf dem bevorzugten Knoten gesichert. Protokollsicherungen können nur von jeweils einer Microsoft Exchange-Instanz auf den vSnap-Server geschrieben werden.

Alle Protokollsicherungsprobleme, die auftreten, werden in den Alertbenachrichtigungen in IBM Spectrum Protect Plus angezeigt.

Exchange-Datenbanken in einer Datenbankverfügbarkeitsgruppe sichern
Sie können die Mailboxdatenbanken in einer Microsoft Exchange-Datenbankverfügbarkeitsgruppe (Database Availability Group = DAG) sichern und angeben, ob die aktive Kopie oder eine passive Kopie der Datenbank für die Sicherung verwendet werden soll. Die Exchange-Server in einer DAG-Umgebung synchronisieren die Daten zwischen aktiven und passiven Kopien für die Hochverfügbarkeit.

Informationen zu diesem Vorgang

Mithilfe der Informationen aus einem Bestandsjob stellt IBM Spectrum Protect Plus eine DAG-Sicht bereit, in der alle Datenbanken in einer Exchange-DAG-Umgebung angezeigt werden. Jede Datenbank hat eine aktive Kopie auf einem Server in der DAG und eine oder mehrere passive Kopien auf den anderen Servern. Standardmäßig werden geplante Sicherungen auf dem Server erstellt, auf dem die Datenbank

aktiv ist, aber Sie können einen anderen Server auswählen, um eine passive Kopie der Datenbank zu sichern.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **Exchange**.
2. Klicken Sie im Fenster **Exchange-Sicherung** auf das Menü **Sicht** und wählen Sie **Datenbankverfügbarkeitsgruppen** aus.
3. Klicken Sie auf die Microsoft Exchange-DAG, die angezeigt werden soll, und wählen Sie dann die Datenbanken aus, die gesichert werden sollen.
4. Klicken Sie auf **Optionen auswählen**. Wählen Sie in der Liste **Bevorzugter Knoten für Sicherung** die Instanz aus, auf der die Sicherungen ausgeführt werden sollen.

   Mit der Option **Bevorzugter Knoten für Sicherung** können Sie eine passive Kopie der Datenbank für die Sicherung auswählen.
5. Klicken Sie auf **SLA-Richtlinie auswählen** und wählen Sie dann eine SLA-Richtlinie aus der Liste aus.
6. Um die Jobdefinition mithilfe von Standardoptionen zu erstellen, klicken Sie auf **Speichern**.

   Die DAG-Datenbanken werden für Sicherungsjobs gemäß der ausgewählten SLA-Richtlinie und dem bevorzugten Knoten geplant.
7. Um die ausgewählte Richtlinie außerhalb des Zeitplans auszuführen, klicken Sie im Fenster **SLA-Richtlinienstatus** auf **Aktionen** > **Starten**.

Strategie der immer inkrementellen Sicherung

IBM Spectrum Protect Plus stellt eine Sicherungsstrategie bereit, die als *immer inkrementell* bezeichnet wird. Bei dieser Sicherungslösung ist keine Planung regelmäßiger Gesamtsicherungsjobs, sondern nur eine einzige erste Gesamtsicherung erforderlich. Danach findet eine fortlaufende Folge von Teilsicherungsjobs statt.

Die Lösung der immer inkrementellen Sicherung hat folgende Vorteile:

- Das im Netz übertragene Datenvolumen wird reduziert.
- Das Datenwachstum wird reduziert, weil alle Teilsicherungen nur die Blöcke enthalten, die sich seit der vorherigen Sicherung geändert haben.
- Die Dauer von Sicherungsjobs wird reduziert.

Der Prozess der immer inkrementellen Sicherung in IBM Spectrum Protect Plus besteht aus den folgenden Schritten:

1. Beim ersten Sicherungsjob wird eine VSS-Momentaufnahme der Exchange-Anwendung erstellt. Die Datenbankdateien befinden sich folglich in einem anwendungskonsistenten Zustand. Die vollständigen Datenbankdateien werden an die vSnap-Position kopiert.
2. Bei allen nachfolgenden Sicherungen wird eine VSS-Momentaufnahme der Exchange-Anwendung erstellt. Die Datenbankdateien befinden sich in einem anwendungskonsistenten Zustand. Es werden jedoch nur die geänderten Blöcke der Datenbankdateien an die vSnap-Position kopiert.
3. Die Sicherungen werden an jedem Zeitpunkt wiederhergestellt, an dem eine Sicherung ausgeführt wird, wodurch es möglich ist, die Datenbank von einem einzigen Sicherungspunkt aus wiederherzustellen.

Microsoft Exchange-Datenbanken zurückschreiben

Wenn Daten in einer Microsoft Exchange-Datenbank verloren gehen oder beschädigt werden, können Sie die Daten aus einer Sicherungskopie zurückschreiben. Definieren Sie mithilfe des Assistenten "Momentaufnahmezurückschreibung" einen Zurückschreibungsjobzeitplan oder eine bedarfsgesteuerte Zurückschreibungsoperation. Sie können einen Job definieren, mit dem Daten in die ursprüngliche Instanz oder in eine alternative Instanz zurückgeschrieben werden; dabei sind verschiedene Typen von Wiederherstellungsoptionen und Konfigurationen verfügbar.

Vorbereitende Schritte
Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Mindestens ein Microsoft Exchange-Sicherungsjob ist definiert und wurde erfolgreich ausgeführt. Anweisungen zum Definieren eines Sicherungsjobs finden Sie in „SLA-Sicherungsjob definieren" auf Seite 171.
- IBM Spectrum Protect Plus-Rollen und -Ressourcengruppen sind dem Benutzer zugeordnet, der den Zurückschreibungsjob definiert. Weitere Informationen zum Zuordnen von Rollen finden Sie in Kapitel 13, „Benutzerzugriff verwalten", auf Seite 311.
- Bei einer Zurückschreibung aus einem IBM Spectrum Protect-Archiv werden Dateien vom Band in einen Staging-Pool migriert, bevor der Job gestartet wird. Abhängig von der Größe der Zurückschreibung kann dieser Prozess mehrere Stunden dauern.

Wichtig: Für Operationen für differenzierte Zurückschreibung müssen Sie sich beim Exchange-Anwendungsserver anmelden und die MMC-GUI (MMC = Microsoft Management Console) verwenden, um Mailboxstapelzurückschreibungstasks und Browser-Tasks für die Mailboxzurückschreibung auszuführen.

Vorgehensweise

Um Daten in einer Microsoft Exchange-Datenbank zurückzuschreiben, führen Sie eine der folgenden Aktionen aus:

- Schreiben Sie eine Datenbank in die ursprüngliche Instanz an die ursprüngliche Position zurück.
- Schreiben Sie eine Datenbank in die ursprüngliche Instanz an eine andere Dateiposition zurück.
- Schreiben Sie eine Datenbank in eine alternative Instanz zurück.
- Schreiben Sie Mailboxdaten mithilfe der Funktion für differenzierte Zurückschreibung zurück.
- Schreiben Sie eine Datenbank in einer Datenbankverfügbarkeitsgruppe (DAG) zurück.

Microsoft Exchange-Datenbank in die ursprüngliche Instanz zurückschreiben
Schreiben Sie eine Microsoft Exchange-Datenbank in ihre ursprüngliche Instanz zurück, indem Sie den Produktionsmodus oder Testmodus verwenden. Sie können auswählen, ob die neueste Sicherung oder eine frühere Version einer Exchange-Datenbanksicherung zurückgeschrieben werden soll.

Vorbereitende Schritte
Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Mindestens ein Microsoft Exchange-Sicherungsjob ist definiert und wurde erfolgreich ausgeführt.
- IBM Spectrum Protect Plus-Rollen und -Ressourcengruppen sind dem Benutzer zugeordnet, der den Zurückschreibungsjob definiert. Weitere Informationen zum Zuordnen von Rollen finden Sie in Kapitel 13, „Benutzerzugriff verwalten", auf Seite 311.

Informationen zu diesem Vorgang
Wenn Sie eine Datenbank an ihre ursprüngliche Position im Produktionsmodus zurückschreiben, können Sie sie nicht umbenennen. Mit dieser Zurückschreibungsoption wird eine vollständige Produktionszurückschreibungsoperation ausgeführt, und die vorhandenen Daten werden an der Zielsite überschrieben.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Exchange-Zurückschreibungsjob zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Exchange** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch öffnen, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **Exchange** klicken.

- Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Informationssymbol im Navigationsfenster des Assistenten.
- Um die optionalen Seiten im Assistenten zu übergehen, wählen Sie **Optionale Schritte überspringen** aus.

2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Schritte aus:
   a) Klicken Sie in der Liste auf eine Quelle, um die Datenbanken anzuzeigen, die für Zurückschreibungsoperationen verfügbar sind. Sie können auch die Suchfunktion verwenden, um nach verfügbaren Instanzen zu suchen, und mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen wechseln.
   b) Klicken Sie auf das Plussymbol neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll. Sie können mehrere Datenbanken aus der Liste auswählen.

      Die ausgewählten Quellen werden der Zurückschreibungsliste neben der Datenbankliste hinzugefügt. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Minussymbol neben dem Eintrag.
   c) Klicken Sie auf **Weiter**, um fortzufahren.
3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der Datenbank an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren.

Option	Beschreibung
Zurückschreibungstyp	Wählen Sie den Typ des Zurückschreibungsjobs aus: **Bedarfsgesteuert: Momentaufnahme** Führt einen einmaligen Zurückschreibungsjob aus einer Datenbankmomentaufnahme aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Bedarfsgesteuert: Zeitpunkt** Führt einen einmaligen Zurückschreibungsjob aus einer Sicherung einer Datenbank nach Zeitpunkt aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Wiederholt auftretend** Erstellt einen sich wiederholenden Job für die Zurückschreibung nach Zeitpunkt, der gemäß einem Zeitplan ausgeführt wird.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position aus, von der Daten zurückgeschrieben werden sollen: **Site** Die Site, an der Momentaufnahmen gesichert wurden. Die Site wird im Fenster **Systemkonfiguration** > **Site** definiert. **Cloudauslagerung** Der Cloud-Server, auf den Momentaufnahmen ausgelagert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Auslagerung** Der Repository-Server, auf den Momentaufnahmen ausgelagert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert. **Cloudarchivierung** Der Cloud-Server, auf dem Momentaufnahmen archiviert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert.

Option	Beschreibung
	Repository-Archivierung Der Repository-Server, auf dem Momentaufnahmen archiviert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus: **Demo** Die Demonstrationssite, von der Momentaufnahmen zurückgeschrieben werden sollen. **Primär** Die primäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. **Sekundär** Die sekundäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, wählen Sie einen Server im Menü **Position auswählen** aus.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datenbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wenn Sie Daten aus einer Cloudressource oder von einem Repository-Server zurückschreiben, wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben; wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert oder in einer Cloudressource oder auf einem Repository-Server archiviert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway auswählen.

4. Wählen Sie auf der Seite **Ziel definieren In ursprüngliche Instanz zurückschreiben** aus und klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite **Zurückschreibungsmethode** eine der folgenden Optionen aus:

   - **Test**. Im Testmodus erstellt der Agent eine neue Datenbank, indem er die Datendateien direkt aus dem vSnap-Repository verwendet. Dieser Zurückschreibungstyp kann für Testzwecke verwendet werden.
   - **Produktion**. Im Produktionsmodus schreibt der Agent zunächst die Dateien vom vSnap-Datenträger in den primären Speicher zurück und erstellt dann unter Verwendung der zurückgeschriebenen Dateien die neue Datenbank.

   Geben Sie nur für die Testzurückschreibung in das Feld **Neuer Datenbankname** den neuen Namen für die zurückgeschriebene Datenbank ein. Das Feld **Neuer Datenbankname** wird auch angezeigt, wenn Sie die Produktionszurückschreibung auswählen, es ist jedoch für die Zurückschreibung an eine neue Datenbankposition in der ursprünglichen Instanz bestimmt. Ausführliche Anweisungen zu dieser Task

finden Sie in „Exchange-Datenbank an eine neue Position in der ursprünglichen Instanz zurückschreiben” auf Seite 179.

6. Optional: Konfigurieren Sie auf der Seite **Joboptionen** weitere Optionen für den Zurückschreibungsjob und klicken Sie auf **Weiter**, um fortzufahren.

   Wiederherstellungsoptionen
   Wählen Sie eine der folgenden Wiederherstellungsoptionen aus:

   Keine Wiederherstellung
   Mit dieser Option wird jede aktualisierende Wiederherstellung nach der Zurückschreibungsoperation übersprungen. Die Datenbank verbleibt in einem Status `Aktualisierende Wiederherstellung anstehend`, bis Sie entscheiden, ob die aktualisierende Wiederherstellung manuell ausgeführt werden soll.

   Bis zum Ende der Sicherung wiederherstellen
   Mit dieser Option wird die ausgewählte Datenbank mit dem Status zum Zeitpunkt der Erstellung der Sicherung zurückgeschrieben.

   Bis zum Ende der verfügbaren Protokolle wiederherstellen
   Mit dieser Option wird die Datenbank zurückgeschrieben und alle verfügbaren Protokolle (einschließlich der Protokolle, die neuer als die Sicherung sind, die möglicherweise auf dem Anwendungsserver vorhanden ist) werden angewendet, um die Datenbank mit dem Stand des letztmöglichen Zeitpunkts wiederherzustellen. Diese Option ist nur verfügbar, wenn Sie **Protokollsicherung aktivieren** im Sicherungsjob ausgewählt haben.

   Bis zu einem bestimmten Zeitpunkt wiederherstellen
   Wenn Protokollsicherungen aktiviert sind, wird mit dieser Option die Datenbank zurückgeschrieben und Protokolle vom Protokollsicherungsdatenträger werden angewendet, um die Datenbank bis zu einem benutzerdefinierten Zwischenzeitpunkt wiederherzustellen. Wählen Sie das Datum und die Uhrzeit über die Optionen für **Nach Zeit** aus.

   Anwendungsoptionen
   Definieren Sie die Anwendungsoptionen:

   Maximale Anzahl paralleler Datenströme pro Datenbank
   Definieren Sie die maximale Anzahl Datenströme pro Datenbank aus dem Sicherungsspeicher. Diese Einstellung gilt für jede Datenbank in der Jobdefinition. Mehrere Datenbanken können auch dann parallel zurückgeschrieben werden, wenn der Wert der Option auf 1 gesetzt wird. Mehrere parallele Datenströme können die Zurückschreibungsgeschwindigkeit verbessern, die Nutzung hoher Bandbreite kann sich jedoch auf die Systemgesamtleistung auswirken.

   Diese Option ist nur gültig, wenn Sie eine Exchange-Datenbank mit ihrem ursprünglichen Datenbanknamen an die ursprüngliche Position zurückschreiben.

   Erweiterte Optionen
   Definieren Sie die erweiterten Jobdefinitionsoptionen:

   Bereinigung direkt beim Fehlschlagen des Jobs ausführen
   Aktivieren Sie diese Option, um zugeordnete Ressourcen automatisch im Rahmen einer Zurückschreibung zu bereinigen, wenn die Wiederherstellung fehlschlägt.

7. Optional: Wählen Sie auf der Seite **Scripts anwenden** das anzuwendende **Vorscript** oder **Nachscript** aus oder wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus. Weitere Informationen zum Arbeiten mit Scripts finden Sie in Scripts konfigurieren. Klicken Sie auf **Weiter**, um fortzufahren.
8. Führen Sie auf der Seite **Zeitplan** eine der folgenden Aktionen aus:
   - Wenn Sie einen bedarfsgesteuerten Job ausführen, klicken Sie auf **Weiter**.
   - Wenn Sie einen sich wiederholenden Job definieren, geben Sie einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an. Klicken Sie auf **Weiter**.
9. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs und klicken Sie auf **Übergeben**, um den Job zu erstellen.

   Der Zurückschreibungsjob wird erstellt; Sie können seinen Status über **Jobs und Operationen** > **Aktive Jobs** überprüfen.

Exchange-Datenbank an eine neue Position in der ursprünglichen Instanz zurückschreiben
Sie können eine Microsoft Exchange-Datenbank in die ursprüngliche Instanz, aber an eine neue Position auf dem Anwendungsserver zurückschreiben. Sie können auswählen, ob die neueste Sicherung oder eine frühere Version einer Exchange-Datenbanksicherung zurückgeschrieben werden soll.

Informationen zu diesem Vorgang
Wenn Sie eine Datenbank mithilfe einer Produktionszurückschreibungsoperation in die ursprüngliche Instanz zurückschreiben, können Sie die Datenbank mit einem neuen Namen für die zurückgeschriebene Datenbank an eine neue Dateiposition auf dem Anwendungsserver zurückschreiben. Im Produktionsmodus schreibt der Agent zunächst die Dateien vom vSnap-Datenträger in den primären Speicher zurück und erstellt dann unter Verwendung der zurückgeschriebenen Dateien eine neue Datenbank.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Exchange-Zurückschreibungsjob zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Exchange** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch öffnen, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **Exchange** klicken.
   - Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Informationssymbol im Navigationsfenster des Assistenten.
   - Um die optionalen Seiten im Assistenten zu übergehen, wählen Sie **Optionale Schritte überspringen** aus.
2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Schritte aus:
   a) Klicken Sie in der Liste auf eine Quelle, um die Datenbanken anzuzeigen, die für Zurückschreibungsoperationen verfügbar sind. Sie können auch die Suchfunktion verwenden, um nach verfügbaren Instanzen zu suchen, und mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen wechseln.

   b) Klicken Sie auf das Plussymbol neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll. Sie können mehrere Datenbanken aus der Liste auswählen.

   Die ausgewählten Quellen werden der Zurückschreibungsliste neben der Datenbankliste hinzugefügt. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Minussymbol neben dem Eintrag.

   c) Klicken Sie auf **Weiter**, um fortzufahren.
3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der Datenbank an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren.

Option	Beschreibung
Zurückschreibungstyp	Wählen Sie den Typ des Zurückschreibungsjobs aus: **Bedarfsgesteuert: Momentaufnahme** Führt einen einmaligen Zurückschreibungsjob aus einer Datenbankmomentaufnahme aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Bedarfsgesteuert: Zeitpunkt** Führt einen einmaligen Zurückschreibungsjob aus einer Sicherung einer Datenbank nach Zeitpunkt aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten.

Option	Beschreibung
	Wiederholt auftretend Erstellt einen sich wiederholenden Job für die Zurückschreibung nach Zeitpunkt, der gemäß einem Zeitplan ausgeführt wird.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position aus, von der Daten zurückgeschrieben werden sollen: **Site** Die Site, an der Momentaufnahmen gesichert wurden. Die Site wird im Fenster **Systemkonfiguration** > **Site** definiert. **Cloudauslagerung** Der Cloud-Server, auf den Momentaufnahmen ausgelagert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Auslagerung** Der Repository-Server, auf den Momentaufnahmen ausgelagert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert. **Cloudarchivierung** Der Cloud-Server, auf dem Momentaufnahmen archiviert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Archivierung** Der Repository-Server, auf dem Momentaufnahmen archiviert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus: **Demo** Die Demonstrationssite, von der Momentaufnahmen zurückgeschrieben werden sollen. **Primär** Die primäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. **Sekundär** Die sekundäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, wählen Sie einen Server im Menü **Position auswählen** aus.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datenbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wenn Sie Daten aus einer Cloudressource oder von einem Repository-Server zurückschreiben, wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben; wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus.

Option	Beschreibung
	Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert oder in einer Cloudressource oder auf einem Repository-Server archiviert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway auswählen.

4. Wählen Sie auf der Seite **Ziel definieren In ursprüngliche Instanz zurückschreiben** aus und klicken Sie auf **Weiter**.
5. Klicken Sie auf der Seite **Zurückschreibungsmethode** auf die Zurückschreibungsoption **Produktion**.

   Tipp: Die Auswahl des Produktionsmodus für diese Zurückschreibungsoperation ist obligatorisch.

   a) Erweitern Sie im Feld **Name** den Datenbanknamen, um die Pfadinformationen für die vorhandene Datenbank auf dem Anwendungsserver anzuzeigen.

   b) Geben Sie in das Feld **Neuer Datenbankname** den neuen Namen für die zurückgeschriebene Datenbank ein.

   c) Fügen Sie im Feld **Zielpfad** die neue Position der Exchange-Datenbankdatei, einschließlich des Namens .edb, und die Protokollposition hinzu.
   Geben Sie beispielsweise für eine Datenbank mit dem Namen Database_A.edb C:\ExchangeDatabase\Database_A\Database_A.edb und für die Position der Protokolle (**Quellenpfad** E01) D:\ExchangeDatabase\Logs\Database_A\ ein.
6. Optional: Konfigurieren Sie auf der Seite **Joboptionen** weitere Optionen für den Zurückschreibungsjob und klicken Sie auf **Weiter**, um fortzufahren.

   Wiederherstellungsoptionen
   Wählen Sie eine der folgenden Wiederherstellungsoptionen aus:

   Keine Wiederherstellung
   Mit dieser Option wird jede aktualisierende Wiederherstellung nach der Zurückschreibungsoperation übersprungen. Die Datenbank verbleibt in einem Status `Aktualisierende Wiederherstellung anstehend`, bis Sie entscheiden, ob die aktualisierende Wiederherstellung manuell ausgeführt werden soll.

   Bis zum Ende der Sicherung wiederherstellen
   Mit dieser Option wird die ausgewählte Datenbank mit dem Status zum Zeitpunkt der Erstellung der Sicherung zurückgeschrieben.

   Bis zum Ende der verfügbaren Protokolle wiederherstellen
   Mit dieser Option wird die Datenbank zurückgeschrieben und alle verfügbaren Protokolle (einschließlich der Protokolle, die neuer als die Sicherung sind, die möglicherweise auf dem Anwendungsserver vorhanden ist) werden angewendet, um die Datenbank mit dem Stand des letztmöglichen Zeitpunkts wiederherzustellen. Diese Option ist nur verfügbar, wenn Sie **Protokollsicherung aktivieren** im Sicherungsjob ausgewählt haben.

   Bis zu einem bestimmten Zeitpunkt wiederherstellen
   Wenn Protokollsicherungen aktiviert sind, wird mit dieser Option die Datenbank zurückgeschrieben und Protokolle vom Protokollsicherungsdatenträger werden angewendet, um die Datenbank bis zu einem benutzerdefinierten Zwischenzeitpunkt wiederherzustellen. Wählen Sie das Datum und die Uhrzeit über die Optionen für **Nach Zeit** aus.

   Anwendungsoptionen
   Definieren Sie die Anwendungsoptionen:

   Maximale Anzahl paralleler Datenströme pro Datenbank
   Definieren Sie die maximale Anzahl Datenströme pro Datenbank aus dem Sicherungsspeicher. Diese Einstellung gilt für jede Datenbank in der Jobdefinition. Mehrere Datenbanken können auch dann parallel zurückgeschrieben werden, wenn der Wert der Option auf 1 gesetzt wird.

Mehrere parallele Datenströme können die Zurückschreibungsgeschwindigkeit verbessern, die Nutzung hoher Bandbreite kann sich jedoch auf die Systemgesamtleistung auswirken.

Diese Option ist nur gültig, wenn Sie eine Exchange-Datenbank mit ihrem ursprünglichen Datenbanknamen an die ursprüngliche Position zurückschreiben.

Erweiterte Optionen
Definieren Sie die erweiterten Jobdefinitionsoptionen:

Bereinigung direkt beim Fehlschlagen des Jobs ausführen
Aktivieren Sie diese Option, um zugeordnete Ressourcen automatisch im Rahmen einer Zurückschreibung zu bereinigen, wenn die Wiederherstellung fehlschlägt.

7. Optional: Wählen Sie auf der Seite **Scripts anwenden** das anzuwendende **Vorscript** oder **Nachscript** aus oder wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus. Weitere Informationen zum Arbeiten mit Scripts finden Sie in Scripts konfigurieren. Klicken Sie auf **Weiter**, um fortzufahren.
8. Führen Sie auf der Seite **Zeitplan** eine der folgenden Aktionen aus:
   - Wenn Sie einen bedarfsgesteuerten Job ausführen, klicken Sie auf **Weiter**.
   - Wenn Sie einen sich wiederholenden Job definieren, geben Sie einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an. Klicken Sie auf **Weiter**.
9. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs und klicken Sie auf **Übergeben**, um den Job zu erstellen.

   Der Zurückschreibungsjob wird erstellt; Sie können seinen Status über **Jobs und Operationen** > **Aktive Jobs** überprüfen.

Microsoft Exchange-Datenbank in eine alternative Instanz zurückschreiben

Sie können eine Microsoft Exchange-Datenbanksicherung auswählen und in eine Exchange Server-Instanz auf einem alternativen Host zurückschreiben. Sie können eine Datenbank im Produktionsmodus oder im Testmodus in die alternative Instanz zurückschreiben.

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Für das Kopieren von Dateien müssen genügend Plattenspeicher und zugeordnete dedizierte Datenträger verfügbar sein.
- Die Dateisystemstruktur auf dem Quellenserver muss mit der Dateisystemstruktur auf dem Zielserver übereinstimmen. Diese Dateisystemstruktur umfasst Tabellenbereiche, Onlineprotokolle und das lokale Datenbankverzeichnis.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Exchange** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch öffnen, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **Exchange** klicken.
   - Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Informationssymbol im Navigationsfenster des Assistenten.
   - Um die optionalen Seiten im Assistenten zu übergehen, wählen Sie **Optionale Schritte überspringen** aus.
2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Schritte aus:
   a) Klicken Sie in der Liste auf eine Quelle, um die Datenbanken anzuzeigen, die für Zurückschreibungsoperationen verfügbar sind. Sie können auch die Suchfunktion verwenden, um nach verfüg-

baren Instanzen zu suchen, und mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen wechseln.

b) Klicken Sie auf das Plussymbol  neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll. Sie können mehrere Datenbanken aus der Liste auswählen.

Die ausgewählten Quellen werden der Zurückschreibungsliste neben der Datenbankliste hinzugefügt. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Minussymbol neben dem Eintrag.

c) Klicken Sie auf **Weiter**, um fortzufahren.

3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der Datenbank an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren.

Option	Beschreibung
Zurückschreibungstyp	Wählen Sie den Typ des Zurückschreibungsjobs aus: **Bedarfsgesteuert: Momentaufnahme** Führt einen einmaligen Zurückschreibungsjob aus einer Datenbankmomentaufnahme aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Bedarfsgesteuert: Zeitpunkt** Führt einen einmaligen Zurückschreibungsjob aus einer Sicherung einer Datenbank nach Zeitpunkt aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Wiederholt auftretend** Erstellt einen sich wiederholenden Job für die Zurückschreibung nach Zeitpunkt, der gemäß einem Zeitplan ausgeführt wird.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position aus, von der Daten zurückgeschrieben werden sollen: **Site** Die Site, an der Momentaufnahmen gesichert wurden. Die Site wird im Fenster **Systemkonfiguration** > **Site** definiert. **Cloudauslagerung** Der Cloud-Server, auf den Momentaufnahmen ausgelagert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Auslagerung** Der Repository-Server, auf den Momentaufnahmen ausgelagert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert. **Cloudarchivierung** Der Cloud-Server, auf dem Momentaufnahmen archiviert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Archivierung** Der Repository-Server, auf dem Momentaufnahmen archiviert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus: **Demo** Die Demonstrationssite, von der Momentaufnahmen zurückgeschrieben werden sollen.

Option	Beschreibung
	Primär Die primäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. **Sekundär** Die sekundäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, wählen Sie einen Server im Menü **Position auswählen** aus.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datenbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wenn Sie Daten aus einer Cloudressource oder von einem Repository-Server zurückschreiben, wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben; wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert oder in einer Cloudressource oder auf einem Repository-Server archiviert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway auswählen.

4. Wählen Sie auf der Seite **Ziel definieren In alternative Instanz zurückschreiben** aus, wählen Sie die Zielinstanz aus, in die die Datenbank zurückgeschrieben werden soll, und klicken Sie dann auf **Weiter**.
5. Wählen Sie auf der Seite **Zurückschreibungsmethode** eine der folgenden Optionen aus:
   - **Test**. Im Testmodus erstellt der Agent eine neue Datenbank, indem er die Datendateien direkt aus dem vSnap-Repository verwendet. Dieser Zurückschreibungstyp kann für Testzwecke verwendet werden.
   - **Produktion**. Im Produktionsmodus schreibt der Agent zunächst die Dateien vom vSnap-Datenträger in den primären Speicher zurück und erstellt dann unter Verwendung der zurückgeschriebenen Dateien die neue Datenbank.

   a) Geben Sie in das Feld **Neuer Datenbankname** einen neuen Datenbanknamen ein.

   b) (Nur Produktionszurückschreibung) Erweitern Sie den Datenbanknamen, um die Pfadinformationen anzuzeigen. Fügen Sie im Feld **Zielpfad** die Position der Exchange-Datenbankdatei auf dem alternativen Host hinzu, einschließlich des .edb-Namens und der Position der Protokolle.

      Geben Sie beispielsweise für eine Datenbank mit dem Namen Database_A.edb C:\ExchangeDatabase\Database_A\Database_A.edb und für die Position der Protokolle c:\ExchangeDatabase\Logs\Database_A\ ein.
6. Optional: Konfigurieren Sie auf der Seite **Joboptionen** weitere Optionen für den Zurückschreibungsjob und klicken Sie auf **Weiter**, um fortzufahren.

   Wiederherstellungsoptionen
   Wählen Sie eine der folgenden Wiederherstellungsoptionen aus:

Keine Wiederherstellung
Mit dieser Option wird jede aktualisierende Wiederherstellung nach der Zurückschreibungsoperation übersprungen. Die Datenbank verbleibt in einem Status `Aktualisierende Wiederherstellung anstehend`, bis Sie entscheiden, ob die aktualisierende Wiederherstellung manuell ausgeführt werden soll.

Bis zum Ende der Sicherung wiederherstellen
Mit dieser Option wird die ausgewählte Datenbank mit dem Status zum Zeitpunkt der Erstellung der Sicherung zurückgeschrieben.

Bis zum Ende der verfügbaren Protokolle wiederherstellen
Mit dieser Option wird die Datenbank zurückgeschrieben und alle verfügbaren Protokolle (einschließlich der Protokolle, die neuer als die Sicherung sind, die möglicherweise auf dem Anwendungsserver vorhanden ist) werden angewendet, um die Datenbank mit dem Stand des letztmöglichen Zeitpunkts wiederherzustellen. Diese Option ist nur verfügbar, wenn Sie **Protokollsicherung aktivieren** im Sicherungsjob ausgewählt haben.

Bis zu einem bestimmten Zeitpunkt wiederherstellen
Wenn Protokollsicherungen aktiviert sind, wird mit dieser Option die Datenbank zurückgeschrieben und Protokolle vom Protokollsicherungsdatenträger werden angewendet, um die Datenbank bis zu einem benutzerdefinierten Zwischenzeitpunkt wiederherzustellen. Wählen Sie das Datum und die Uhrzeit über die Optionen für **Nach Zeit** aus.

Anwendungsoptionen
Definieren Sie die Anwendungsoptionen:

Maximale Anzahl paralleler Datenströme pro Datenbank
Definieren Sie die maximale Anzahl Datenströme pro Datenbank aus dem Sicherungsspeicher. Diese Einstellung gilt für jede Datenbank in der Jobdefinition. Mehrere Datenbanken können auch dann parallel zurückgeschrieben werden, wenn der Wert der Option auf 1 gesetzt wird. Mehrere parallele Datenströme können die Zurückschreibungsgeschwindigkeit verbessern, die Nutzung hoher Bandbreite kann sich jedoch auf die Systemgesamtleistung auswirken.

Diese Option ist nur gültig, wenn Sie eine Exchange-Datenbank mit ihrem ursprünglichen Datenbanknamen an die ursprüngliche Position zurückschreiben.

Erweiterte Optionen
Definieren Sie die erweiterten Jobdefinitionsoptionen:

Bereinigung direkt beim Fehlschlagen des Jobs ausführen
Aktivieren Sie diese Option, um zugeordnete Ressourcen automatisch im Rahmen einer Zurückschreibung zu bereinigen, wenn die Wiederherstellung fehlschlägt.

7. Optional: Wählen Sie auf der Seite **Scripts anwenden** das anzuwendende **Vorscript** oder **Nachscript** aus oder wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus. Weitere Informationen zum Arbeiten mit Scripts finden Sie in Scripts konfigurieren. Klicken Sie auf **Weiter**, um fortzufahren.
8. Führen Sie auf der Seite **Zeitplan** eine der folgenden Aktionen aus:
   - Wenn Sie einen bedarfsgesteuerten Job ausführen, klicken Sie auf **Weiter**.
   - Wenn Sie einen sich wiederholenden Job definieren, geben Sie einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an. Klicken Sie auf **Weiter**.
9. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs und klicken Sie auf **Übergeben**, um den Job zu erstellen.

   Der Zurückschreibungsjob wird erstellt; Sie können seinen Status über **Jobs und Operationen** > **Aktive Jobs** überprüfen.

Einzelne Mailboxeinträge mithilfe einer Operation für differenzierte Zurückschreibung zurückschreiben

Sie können einzelne Microsoft Exchange-Mailboxeinträge mithilfe einer Operation für differenzierte Zurückschreibung und der IBM Spectrum Protect Plus-MMC-GUI (MMC = Microsoft Management Console) zurückschreiben.

Vorbereitende Schritte
Sie müssen über RBAC-Berechtigungen (RBAC = Role-Based Access Control) verfügen, um Operationen für die Zurückschreibung einer einzelnen Mailbox auszuführen. Wurden keine RBAC-Berechtigungen zugeordnet, können in der IBM Spectrum Protect Plus-MMC-GUI für jede fehlende Rolle Konfigurationsfehler auftreten.

Tipp:

Werden rollenbasierte Konfigurationsfehler in der IBM Spectrum Protect Plus-MMC-GUI festgestellt, können Sie die erforderlichen Berechtigungen manuell definieren, um die Fehler zu beheben (siehe „Berechtigungen" auf Seite 168), oder Sie können den IBM Spectrum Protect Plus-Konfigurationsassistenten ausführen, um automatisch Berechtigungen zu konfigurieren (siehe Schritt „14" auf Seite 189).

Informationen zu diesem Vorgang

Um eine Operation für differenzierte Zurückschreibung zu starten, führen Sie die vorbereitenden Schritte in der IBM Spectrum Protect Plus-GUI aus und melden Sie sich dann beim Exchange-Anwendungsserver an. Verwenden Sie dann die IBM Spectrum Protect Plus-MMC-GUI, um Benutzermailboxdaten aus der Wiederherstellungsdatenbank zurückzuschreiben, die von der Operation für differenzierte Zurückschreibung erstellt wird. Eine Operation für differenzierte Zurückschreibung kann verwendet werden, um die folgenden Tasks auszuführen:

- Sie können ausgewählte Mailboxeinträge in die ursprüngliche Mailbox, in eine andere Online-Mailbox auf demselben Server oder in eine Unicode-PST-Datei zurückschreiben.
- Sie können eine Datenbank mit Mailboxen für öffentliche Ordner, eine Mailbox für öffentliche Ordner oder nur einen Teil der Mailbox, wie beispielsweise einen bestimmten öffentlichen Ordner, zurückschreiben.
- Sie können eine Archivmailbox oder einen Teil der Mailbox, wie beispielsweise einen bestimmten Ordner, zurückschreiben.
- Sie können Archivmailboxnachrichten in eine Mailbox, die sich auf dem Exchange Server befindet, in eine Archivmailbox oder in eine Exchange Server-PST-Datei zurückschreiben.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Exchange** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch öffnen, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **Exchange** klicken.
   - Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Informationssymbol im Navigationsfenster des Assistenten.
   - Um die optionalen Seiten im Assistenten zu übergehen, wählen Sie **Optionale Schritte überspringen** aus.
2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Schritte aus:
   a) Klicken Sie in der Liste auf eine Quelle, um die Datenbanken anzuzeigen, die für Zurückschreibungsoperationen verfügbar sind. Sie können auch die Suchfunktion verwenden, um nach verfügbaren Instanzen zu suchen, und mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen wechseln.

   b) Klicken Sie auf das Plussymbol neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll.

   Tipp: Für eine Operation für differenzierte Zurückschreibung dürfen Sie nur eine einzige Datenbank auswählen. Wenn Sie mehrere Datenbanken auswählen, ist die Option für die differenzierte Zurückschreibung auf der Seite **Zurückschreibungsmethode** nicht verfügbar.

Die ausgewählte Quelle wird der Zurückschreibungsliste neben der Datenbankliste hinzugefügt.

Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Minussymbol  neben dem Eintrag.

c) Klicken Sie auf **Weiter**, um fortzufahren.

3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der Datenbank an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren.

Option	Beschreibung
Zurückschreibungstyp	Wählen Sie den Typ des Zurückschreibungsjobs aus: **Bedarfsgesteuert: Momentaufnahme** Führt einen einmaligen Zurückschreibungsjob aus einer Datenbankmomentaufnahme aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Bedarfsgesteuert: Zeitpunkt** Führt einen einmaligen Zurückschreibungsjob aus einer Sicherung einer Datenbank nach Zeitpunkt aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Wiederholt auftretend** Erstellt einen sich wiederholenden Job für die Zurückschreibung nach Zeitpunkt, der gemäß einem Zeitplan ausgeführt wird.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position aus, von der Daten zurückgeschrieben werden sollen: **Site** Die Site, an der Momentaufnahmen gesichert wurden. Die Site wird im Fenster **Systemkonfiguration** > **Site** definiert. **Cloudauslagerung** Der Cloud-Server, auf den Momentaufnahmen ausgelagert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Auslagerung** Der Repository-Server, auf den Momentaufnahmen ausgelagert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert. **Cloudarchivierung** Der Cloud-Server, auf dem Momentaufnahmen archiviert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Archivierung** Der Repository-Server, auf dem Momentaufnahmen archiviert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus: **Demo** Die Demonstrationssite, von der Momentaufnahmen zurückgeschrieben werden sollen. **Primär** Die primäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen.

Option	Beschreibung
	Sekundär Die sekundäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, wählen Sie einen Server im Menü **Position auswählen** aus.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datenbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wenn Sie Daten aus einer Cloudressource oder von einem Repository-Server zurückschreiben, wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben; wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert oder in einer Cloudressource oder auf einem Repository-Server archiviert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway auswählen.

4. Wählen Sie auf der Seite **Ziel definieren In ursprüngliche Instanz zurückschreiben** aus und klicken Sie auf **Weiter**.
5. Klicken Sie auf der Seite **Zurückschreibungsmethode** auf **Differenzierte Zurückschreibung**.

   Der Name der Wiederherstellungsdatenbank wird im Feld **Neuer Datenbankname** angezeigt. Der Name besteht aus dem vorhandenen Datenbanknamen mit dem Suffix _RDB.
6. Optional: Auf der Seite **Joboptionen** sind **Bis zum Ende der Sicherung wiederherstellen** und **Bereinigung direkt beim Fehlschlagen des Jobs ausführen** standardmäßig ausgewählt. Klicken Sie auf **Weiter**, um fortzufahren.
7. Optional: Wählen Sie auf der Seite **Scripts anwenden** das anzuwendende **Vorscript** oder **Nachscript** aus oder wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus. Weitere Informationen zum Arbeiten mit Scripts finden Sie in Scripts konfigurieren. Klicken Sie auf **Weiter**, um fortzufahren.
8. Führen Sie auf der Seite **Zeitplan** eine der folgenden Aktionen aus:
   - Wenn Sie einen bedarfsgesteuerten Job ausführen, klicken Sie auf **Weiter**.
   - Wenn Sie einen sich wiederholenden Job definieren, geben Sie einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an. Klicken Sie auf **Weiter**.
9. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs und klicken Sie auf **Übergeben**, um den Job zu erstellen.

   Der Zurückschreibungsjob wird erstellt; Sie können seinen Status über **Jobs und Operationen** > **Aktive Jobs** überprüfen.
10. Klicken Sie im Navigationsfenster auf **Jobs und Operationen** > **Aktive Ressourcen**, um die Wiederherstellungsdatenbank und Details zum Mountpunkt anzuzeigen.

    Tipp: Klicken Sie auf das Symbol  , um eine Informationsnachricht anzuzeigen, die die nächsten Schritte für die Ausführung der Task für differenzierte Zurückschreibung beschreibt.

11. Stellen Sie die Verbindung zur Exchange-Anwendungsserverinstanz her, indem Sie die Remotedesktopverbindung (Remote Desktop Connection = RDC) oder Virtual Network Computing (VNC) verwenden, wenn die Herstellung der Verbindung über Fernzugriff erfolgt, oder indem Sie sich lokal bei der Exchange Server-Maschine anmelden.

    Mit der Operation für differenzierte Zurückschreibung wird die IBM Spectrum Protect Plus-MMC-GUI automatisch auf dem Anwendungsserver installiert und gestartet. Wenn der Start der MMC-GUI fehlschlägt, starten Sie die GUI manuell, indem Sie den Pfad verwenden, der in der Informationsnachricht für **Aktive Ressourcen** angegeben ist.
12. Klicken Sie in der IBM Spectrum Protect Plus-MMC-GUI auf den Knoten **Daten schützen und wiederherstellen** und wählen Sie **Exchange Server** aus.
13. Klicken Sie auf der Registerkarte **Wiederherstellen** für die Exchange Server-Instanz auf **Anzeigen** > **Browser für Mailboxzurückschreibung**, um die Mailbox aus der Wiederherstellungsdatenbank anzuzeigen.
14. Optional: Führen Sie den IBM Spectrum Protect Plus-Konfigurationsassistenten aus:
    a) Klicken Sie im Navigationsfenster auf **Dashboard** > **Verwalten** > **Konfiguration** > **Assistenten** > **IBM Spectrum Protect Plus Konfiguration**.
    b) Klicken Sie im Fenster **Aktionen** auf **Starten**.

       Der Konfigurationsassistent führt die Prüfung der Voraussetzungen aus.
    c) Wenn die Prüfung der Voraussetzungen ausgeführt wurde, klicken Sie auf den Link **Warnungen** neben **Prüfung der Benutzerrollen**.
    d) Klicken Sie im Nachrichtendialogfenster auf **Ja**, um alle fehlenden Rollen hinzuzufügen.
    e) Klicken Sie im Konfigurationsassistenten auf **Weiter** und klicken Sie dann auf **Fertigstellen**.
15. Klicken Sie in der Baumstruktur **Browser für Mailboxzurückschreibung > Quelle** auf die Mailbox, die die zurückzuschreibenden Einträge enthält. Damit wird es Ihnen ermöglicht, die einzelnen Ordner und Nachrichten zu durchsuchen.

    Wählen Sie eine der folgenden Aktionen aus, um den Ordner oder die Nachricht auszuwählen, der bzw. die zurückgeschrieben werden soll.

Tabelle 19. Voranzeige und Filterung von Mailboxeinträgen

Task	**Aktion**
Mailboxeinträge voranzeigen	a. Wählen Sie einen Mailboxeintrag aus, wie beispielsweise **Posteingang**, um seinen Inhalt im Voranzeigefenster anzuzeigen. b. Klicken Sie auf einen einzelnen Eintrag im Voranzeigefenster, wie beispielsweise eine E-Mail-Nachricht, um den Nachrichtentext und die Details anzuzeigen. c. Wenn ein Eintrag eine Anlage enthält, klicken Sie auf das Anlagensymbol, um den Inhalt der Anlage anzuzeigen.

Tabelle 19. Voranzeige und Filterung von Mailboxeinträgen (Forts.)	
Task	**Aktion**
Mailboxeinträge filtern	Mit den Filteroptionen können Sie die Liste der Ordner und Nachrichten, die zurückgeschrieben werden sollen, eingrenzen: a. Klicken Sie auf **Filteroptionen anzeigen** und **Zeile hinzufügen**. b. Klicken Sie auf den Abwärtspfeil im Feld **Spaltenname** und wählen Sie einen Eintrag zum Filtern aus. Sie können nach Ordnernamen, Betrefftext und anderen Optionen filtern. **Einschränkung:** Ordner für öffentliche Mailboxen können nur anhand der Spalte **Ordnername** gefiltert werden. Wenn Sie **Gesamter Inhalt** auswählen, werden die Mailboxeinträge nach Anlagennamen, Absender, Betreff und Nachrichtentext gefiltert. c. Wählen Sie im Feld **Operator** einen Operator aus: Enthält. d. Geben Sie im Feld **Wert** einen Filterwert an. e. Um zusätzliche Filterkriterien anzugeben, klicken Sie auf **Zeile hinzufügen**. f. Klicken Sie auf **Filter anwenden**, um die Nachrichten und Ordner zu filtern.

16. Wenn Sie den Mailboxeintrag ausgewählt haben, der zurückgeschrieben werden soll, klicken Sie im Fenster **Aktionen** auf die Zurückschreibungstask, die ausgeführt werden soll. Wählen Sie eine der folgenden Optionen aus:

    - **Ordner in ursprüngliche Mailbox zurückschreiben**
    - **Nachrichten in ursprüngliche Mailbox zurückschreiben**
    - **E-Mail-Nachrichteninhalt speichern**

    Tipp: Wenn Sie auf **E-Mail-Nachrichteninhalt speichern** klicken, wird ein Windows-Fenster "Datei speichern" angezeigt. Geben Sie die Position und den Nachrichtennamen an und klicken Sie auf **Speichern**.

    Wenn Sie die Zurückschreibungsoption auswählen, wird das Fenster **Zurückschreibungsfortschritt** geöffnet. Es zeigt den Fortschritt der Zurückschreibungsoperation an und zeigt an, wenn der Mailboxeintrag zurückgeschrieben wurde.

17. Führen Sie die folgenden Schritte aus, um einen Mailboxeintrag in eine andere Mailbox oder PST-Datei zurückzuschreiben.

    Anmerkung: Sie können auch eine vollständige Mailbox in eine andere Mailbox oder PST-Datei zurückschreiben.

    Wählen Sie eine Aktion aus der folgenden Tabelle aus:

Tabelle 20. Mailboxeintrag in eine andere Mailbox oder PST-Datei zurückschreiben

Task	Aktion
Mailboxeintrag (oder Mailbox) in eine andere Mailbox zurückschreiben	a. Klicken Sie im Fenster **Aktionen** auf **Exchange-Mailbox öffnen**. b. Geben Sie den Aliasnamen der Mailbox ein, um sie als Zurückschreibungsziel anzugeben. c. Ziehen Sie den Quellenmailboxeintrag (oder die Quellenmailbox) auf die Zielmailbox im Fenster "Ergebnisse". **Einschränkung:** Sie können E-Mail-Einträge oder Unterordner im Ordner `Wiederherstellbare Elemente` nicht auf eine Zielmailbox ziehen.
Mailboxeintrag (oder Mailbox) in eine Datei für persönliche Ordner von Outlook (`.pst`) zurückschreiben	a. Klicken Sie im Fenster **Aktionen** auf **Nicht-Unicode-PST-Datei öffnen**. b. Wenn das Fenster **Datei öffnen** geöffnet wird, wählen Sie eine vorhandene PST-Datei aus oder erstellen Sie eine PST-Datei. c. Ziehen Sie den Quellenmailboxeintrag (oder die Quellenmailbox) auf die PST-Zieldatei im Fenster "Ergebnisse". **Einschränkung:** Sie können die Sicht **Browser für Mailboxzurückschreibung** nur mit Nicht-Unicode-PST-Dateien verwenden.

Tabelle 20. Mailboxeintrag in eine andere Mailbox oder PST-Datei zurückschreiben (Forts.)

Task	Aktion
Öffentlichen Ordner zurückschreiben	Wählen Sie diese Aktion aus, um einen öffentlichen Ordner in eine vorhandene Mailbox für öffentliche Onlineordner zurückzuschreiben. Sie können die Mailbox filtern und einen bestimmten öffentlichen Ordner in einen vorhandenen öffentlichen Onlineordner zurückschreiben. Geben Sie in das Feld **Zurückzuschreibender Ordner** den Namen des öffentlichen Ordners ein, der zurückgeschrieben werden soll. • Um einen Unterordner in einen übergeordneten Ordner zurückzuschreiben, geben Sie den vollständigen Ordnerpfad in diesem Format an: *Name_des_übergeordneten_Ordners*/*Name_des_Unterordners*. • Um alle Unterordner in einen übergeordneten Ordner zurückzuschreiben, verwenden Sie *Name_des_übergeordneten_Ordners*/*. • Wenn der vollständige Ordnerpfad Leerzeichen enthält, schließen Sie den Ordnerpfad in Anführungszeichen ein und hängen Sie keinen umgekehrten Schrägstrich (\) an. Sie können einen öffentlichen Ordner auch ganz oder teilweise in eine andere Mailbox für öffentliche Ordner als die ursprüngliche Mailbox zurückschreiben. Geben Sie im Feld **Zielmailbox für öffentliche Ordner** die Zielmailbox für öffentliche Ordner an, in die die Zurückschreibung erfolgen soll.

18. Klicken Sie im Fenster **Aktionen** auf **Exchange-Mailbox schließen** oder **PST-Datei schließen**, um die Zielmailbox oder PST-Datei zu schließen.

    Tipp: Sie können MMC (Microsoft Management Console) aktivieren, um Diagnoseinformationen zu sammeln, die Sie bei der Bestimmung von Problemen mit Zurückschreibungsoperationen unterstützen. Im Rahmen des Prozesses werden Konfigurationsdateien, Tracedateien und allgemeine Diagnoseinformationen der MMC-GUI gesammelt. Weitere Informationen finden Sie in der folgenden Technote: Enabling diagnostic information in the IBM Spectrum Protect Plus MMC GUI(http://www.ibm.com/support/docview.wss?uid=ibm10882270).
19. Wenn die Zurückschreibungsoperation für die einzelnen Einträge beendet ist, kehren Sie zu IBM Spectrum Protect Plus zurück. Klicken Sie im Fenster **Jobs und Operationen** > **Aktive Ressourcen** auf **Aktionen** > **Differenzierte Zurückschreibung abbrechen**, um den Prozess der differenzierten Zurückschreibung zu beenden.

Mailboxen mithilfe einer Operation für differenzierte Zurückschreibung zurückschreiben
Sie können Microsoft Exchange-Mailboxen mithilfe einer Operation für differenzierte Zurückschreibung und der IBM Spectrum Protect Plus-MMC-GUI (MMC = Microsoft Management Console) zurückschreiben.

Vorbereitende Schritte
Sie müssen über RBAC-Berechtigungen (RBAC = Role-Based Access Control) verfügen, um Operationen für die Zurückschreibung einer einzelnen Mailbox auszuführen. Wurden keine RBAC-Berechtigungen zugeordnet, können in der IBM Spectrum Protect Plus-MMC-GUI für jede fehlende Rolle Konfigurationsfehler auftreten.

Tipp:

Werden rollenbasierte Konfigurationsfehler in der IBM Spectrum Protect Plus-MMC-GUI festgestellt, können Sie die erforderlichen Berechtigungen manuell definieren, um die Fehler zu beheben (siehe „Berechtigungen" auf Seite 168), oder Sie können den IBM Spectrum Protect Plus-Konfigurationsassistenten ausführen, um automatisch Berechtigungen zu konfigurieren (siehe Schritt „14" auf Seite 196).

Informationen zu diesem Vorgang

Um eine Operation für differenzierte Zurückschreibung zu starten, führen Sie die vorbereitenden Schritte in der IBM Spectrum Protect Plus-GUI aus und melden Sie sich dann beim Exchange-Anwendungsserver an. Verwenden Sie dann die IBM Spectrum Protect Plus-MMC-GUI, um Benutzermailboxdaten aus der Wiederherstellungsdatenbank zurückzuschreiben, die von der Operation für differenzierte Zurückschreibung erstellt wird. Eine Operation für differenzierte Zurückschreibung kann verwendet werden, um die folgenden Tasks auszuführen:

- Sie können eine vollständige Mailbox oder ausgewählte Mailboxeinträge in die ursprüngliche Mailbox, in eine andere Online-Mailbox auf demselben Server oder in eine Unicode-PST-Datei zurückschreiben.
- Sie können eine Datenbank mit Mailboxen für öffentliche Ordner, eine Mailbox für öffentliche Ordner oder nur einen Teil der Mailbox, wie beispielsweise einen bestimmten öffentlichen Ordner, zurückschreiben.
- Sie können eine Archivmailbox oder einen Teil der Mailbox, wie beispielsweise einen bestimmten Ordner, zurückschreiben.
- Sie können Archivmailboxnachrichten in eine Mailbox, die sich auf dem Exchange Server befindet, in eine Archivmailbox oder in eine Exchange Server-PST-Datei zurückschreiben.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Exchange** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch öffnen, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **Exchange** klicken.
   - Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Informationssymbol im Navigationsfenster des Assistenten.
   - Um die optionalen Seiten im Assistenten zu übergehen, wählen Sie **Optionale Schritte überspringen** aus.
2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Schritte aus:
   a) Klicken Sie in der Liste auf eine Quelle, um die Datenbanken anzuzeigen, die für Zurückschreibungsoperationen verfügbar sind. Sie können auch die Suchfunktion verwenden, um nach verfügbaren Instanzen zu suchen, und mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen wechseln.

   b) Klicken Sie auf das Plussymbol neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll.

   Tipp: Für eine Operation für differenzierte Zurückschreibung dürfen Sie nur eine einzige Datenbank auswählen. Wenn Sie mehrere Datenbanken auswählen, ist die Option für die differenzierte Zurückschreibung auf der Seite **Zurückschreibungsmethode** nicht verfügbar.

   Die ausgewählte Quelle wird der Zurückschreibungsliste neben der Datenbankliste hinzugefügt.

   Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Minussymbol neben dem Eintrag.

   c) Klicken Sie auf **Weiter**, um fortzufahren.

3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der Datenbank an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren.

Option	Beschreibung
Zurückschreibungstyp	Wählen Sie den Typ des Zurückschreibungsjobs aus: **Bedarfsgesteuert: Momentaufnahme** Führt einen einmaligen Zurückschreibungsjob aus einer Datenbankmomentaufnahme aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Bedarfsgesteuert: Zeitpunkt** Führt einen einmaligen Zurückschreibungsjob aus einer Sicherung einer Datenbank nach Zeitpunkt aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Wiederholt auftretend** Erstellt einen sich wiederholenden Job für die Zurückschreibung nach Zeitpunkt, der gemäß einem Zeitplan ausgeführt wird.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position aus, von der Daten zurückgeschrieben werden sollen: **Site** Die Site, an der Momentaufnahmen gesichert wurden. Die Site wird im Fenster **Systemkonfiguration** > **Site** definiert. **Cloudauslagerung** Der Cloud-Server, auf den Momentaufnahmen ausgelagert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Auslagerung** Der Repository-Server, auf den Momentaufnahmen ausgelagert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert. **Cloudarchivierung** Der Cloud-Server, auf dem Momentaufnahmen archiviert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Archivierung** Der Repository-Server, auf dem Momentaufnahmen archiviert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus: **Demo** Die Demonstrationssite, von der Momentaufnahmen zurückgeschrieben werden sollen. **Primär** Die primäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. **Sekundär** Die sekundäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, wählen Sie einen Server im Menü **Position auswählen** aus.

Option	Beschreibung
Datumsauswahl	Geben Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datenbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wenn Sie Daten aus einer Cloudressource oder von einem Repository-Server zurückschreiben, wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben; wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert oder in einer Cloudressource oder auf einem Repository-Server archiviert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway auswählen.

4. Wählen Sie auf der Seite **Ziel definieren In ursprüngliche Instanz zurückschreiben** aus und klicken Sie auf **Weiter**.
5. Klicken Sie auf der Seite **Zurückschreibungsmethode** auf **Differenzierte Zurückschreibung**.

   Der Name der Wiederherstellungsdatenbank wird im Feld **Neuer Datenbankname** angezeigt. Der Name besteht aus dem vorhandenen Datenbanknamen mit dem Suffix _RDB.
6. Optional: Auf der Seite **Joboptionen** sind **Bis zum Ende der Sicherung wiederherstellen** und **Bereinigung direkt beim Fehlschlagen des Jobs ausführen** standardmäßig ausgewählt. Klicken Sie auf **Weiter**, um fortzufahren.
7. Optional: Wählen Sie auf der Seite **Scripts anwenden** das anzuwendende **Vorscript** oder **Nachscript** aus oder wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus. Weitere Informationen zum Arbeiten mit Scripts finden Sie in Scripts konfigurieren. Klicken Sie auf **Weiter**, um fortzufahren.
8. Führen Sie auf der Seite **Zeitplan** eine der folgenden Aktionen aus:
   - Wenn Sie einen bedarfsgesteuerten Job ausführen, klicken Sie auf **Weiter**.
   - Wenn Sie einen sich wiederholenden Job definieren, geben Sie einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an. Klicken Sie auf **Weiter**.
9. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs und klicken Sie auf **Übergeben**, um den Job zu erstellen.

   Der Zurückschreibungsjob wird erstellt; Sie können seinen Status über **Jobs und Operationen** > **Aktive Jobs** überprüfen.
10. Klicken Sie im Navigationsfenster auf **Jobs und Operationen** > **Aktive Ressourcen**, um die Wiederherstellungsdatenbank und Details zum Mountpunkt anzuzeigen.

    Tipp: Klicken Sie auf das Symbol , um eine Informationsnachricht anzuzeigen, die die nächsten Schritte für die Ausführung der Task für differenzierte Zurückschreibung beschreibt.
11. Stellen Sie die Verbindung zur Exchange-Anwendungsserverinstanz her, indem Sie die Remotedesktopverbindung (Remote Desktop Connection = RDC) oder Virtual Network Computing (VNC) verwenden, wenn die Herstellung der Verbindung über Fernzugriff erfolgt, oder indem Sie sich lokal bei der Exchange Server-Maschine anmelden.

    Mit der Operation für differenzierte Zurückschreibung wird die IBM Spectrum Protect Plus-MMC-GUI automatisch auf dem Anwendungsserver installiert und gestartet. Wenn der Start der MMC-GUI fehl-

schlägt, starten Sie die GUI manuell, indem Sie den Pfad verwenden, der in der Informationsnachricht für **Aktive Ressourcen** angegeben ist.

12. Klicken Sie in der IBM Spectrum Protect Plus-MMC-GUI auf den Knoten **Daten schützen und wiederherstellen** und wählen Sie **Exchange Server** aus.
13. Wählen Sie auf der Registerkarte **Wiederherstellen** für die Exchange Server-Instanz **Sicht** > **Mailboxzurückschreibung** aus.

    Eine Liste der Benutzermailboxen aus allen Datenbanken, die in der Sicherung eingeschlossen sind, wird angezeigt.
14. Optional: Führen Sie den IBM Spectrum Protect Plus-Konfigurationsassistenten aus:
    a) Klicken Sie im Navigationsfenster auf **Dashboard** > **Verwalten** > **Konfiguration** > **Assistenten** > **IBM Spectrum Protect Plus Konfiguration**.
    b) Klicken Sie im Fenster **Aktionen** auf **Starten**.

       Der Konfigurationsassistent führt die Prüfung der Voraussetzungen aus.
    c) Wenn die Prüfung der Voraussetzungen ausgeführt wurde, klicken Sie auf den Link **Warnungen** neben **Prüfung der Benutzerrollen**.
    d) Klicken Sie im Nachrichtendialogfenster auf **Ja**, um alle fehlenden Rollen hinzuzufügen.
    e) Klicken Sie im Konfigurationsassistenten auf **Weiter** und klicken Sie dann auf **Fertigstellen**.
15. Wählen Sie eine oder mehrere Mailboxen aus der Wiederherstellungsdatenbank für die Zurückschreibung aus. Mailboxen werden nach Mailboxnamen, Aliasnamen, Server, Datenbank und Mailboxtyp aufgelistet.

    Sie können nur Benutzermailboxen zurückschreiben, die sich in der Wiederherstellungsdatenbank befinden.

    Tipp: Mailboxen aus anderen Datenbanken werden nur zu Informationszwecken in dieser Sicht angezeigt. Befindet sich die Datenbank, die zurückgeschrieben werden soll, nicht in der Wiederherstellungsdatenbank, verwenden Sie diese Sicht, um zu bestimmen, welcher Exchange-Datenbank die Benutzermailbox zugeordnet war. Sie können dann die Task für die differenzierte Zurückschreibung für diese Datenbank erneut ausführen.
16. Um die Zurückschreibungsoperation auszuführen, klicken Sie im Fenster **Aktionen** auf eine der folgenden Zurückschreibungsoptionen.

Tabelle 21. Zurückschreibungsoptionen

Option	**Aktion**
E-Mail an ursprüngliche Position zurückschreiben	Wählen Sie diese Option aus, um E-Mail-Einträge an ihre Position zum Zeitpunkt der Sicherungsoperation zurückzuschreiben.
E-Mail an alternative Position zurückschreiben	Wählen Sie diese Option aus, um die E-Mail-Einträge in eine andere Mailbox zurückzuschreiben. • Geben Sie im Fenster **Optionen für alternative Mailbox** den **Aliasnamen der Mailbox** ein. **Tipp:** Wenn gelöschte E-Mail-Einträge oder Tasks im Ordner `Wiederherstellbare Elemente` einer Mailbox markiert sind, werden die Einträge mit dem Flagattribut in die Sicht **Gekennzeichnete Elemente und Aufgaben** in der Zielmailbox zurückgeschrieben.

Tabelle 21. Zurückschreibungsoptionen (Forts.)

Option	Aktion
E-Mail in Nicht-Unicode-PST-Datei zurückschreiben **Einschränkung:** • Diese Option ist nur für Exchange Server 2013 verfügbar. • Jeder Ordner kann maximal 16.383 E-Mail-Einträge enthalten.	Wählen Sie diese Option aus, um E-Mail-Einträge in eine Nicht-Unicode-PST-Datei (Persönliche Ordner-Datei mit der Erweiterung `.pst`) zurückzuschreiben. Wenn E-Mail-Einträge in eine PST-Datei zurückgeschrieben werden und eine einzelne Mailbox ausgewählt wurde, werden Sie zur Eingabe eines Dateinamens aufgefordert. Wenn E-Mail-Einträge in eine PST-Datei zurückgeschrieben werden und mehrere Mailboxen ausgewählt wurden, werden Sie zur Eingabe einer Verzeichnisposition aufgefordert. Jede Mailbox wird in eine separate PST-Datei zurückgeschrieben, die den Namen der Mailbox in dem angegebenen Verzeichnis wiedergibt. Wenn die PST-Datei vorhanden ist, wird diese Datei verwendet. Andernfalls wird die Datei erstellt.
E-Mail in Unicode-PST-Datei zurückschreiben	Wählen Sie diese Option aus, um E-Mail-Einträge in eine Unicode-PST-Datei zurückzuschreiben. Wenn E-Mail-Einträge in eine PST-Datei zurückgeschrieben werden und eine einzelne Mailbox ausgewählt wurde, werden Sie zur Eingabe eines Dateinamens aufgefordert. Wenn E-Mail-Einträge in eine PST-Datei zurückgeschrieben werden und mehrere Mailboxen ausgewählt wurden, werden Sie zur Eingabe einer Verzeichnisposition aufgefordert. **Tipp:** Sie können einen Standardpfadnamen (z. B. `c:\PST\mailbox.pst`) oder einen UNC-Pfad (z. B. `\\server\c$\PST\mailbox.pst`) eingeben. Wenn Sie einen Standardpfad eingeben, wird der Pfad in einen UNC-Pfad konvertiert. Ist der UNC-Pfad ein vom Standard abweichender UNC-Pfad, geben Sie den UNC-Pfad direkt ein. Jede Mailbox wird in eine separate PST-Datei zurückgeschrieben, die den Namen der Mailbox in dem angegebenen Verzeichnis wiedergibt. Wenn die PST-Datei vorhanden ist, wird diese Datei verwendet. Andernfalls wird die Datei erstellt.

Tabelle 21. Zurückschreibungsoptionen (Forts.)

Option	Aktion
Mailbox für öffentliche Ordner zurückschreiben	Wählen Sie diese Option aus, um eine Mailbox für öffentliche Ordner in eine Mailbox für öffentliche Onlineordner zurückzuschreiben. Geben Sie in das Feld **Zurückzuschreibender Ordner** den Namen des öffentlichen Ordners ein, der zurückgeschrieben werden soll: • Um einen Unterordner in einen übergeordneten Ordner zurückzuschreiben, geben Sie den vollständigen Ordnerpfad in diesem Format an: *Name_des_übergeordneten_Ordners/Name_des_Unterordners*. • Um alle Unterordner in einen übergeordneten Ordner zurückzuschreiben, verwenden Sie *Name_des_übergeordneten_Ordners/**. • Wenn der vollständige Ordnerpfad Leerzeichen enthält, schließen Sie den Ordnerpfad in Anführungszeichen ein und hängen Sie keinen umgekehrten Schrägstrich (\) an. Sie können auch eine Mailbox für öffentliche Ordner ganz oder teilweise in eine andere Mailbox für öffentliche Ordner als die ursprüngliche Mailbox zurückschreiben. Geben Sie im Feld **Zielmailbox für öffentliche Ordner** die Zielmailbox für öffentliche Ordner an.
E-Mail in Archivmailbox zurückschreiben	Diese Option gilt für eine primäre Mailbox oder eine Archivmailbox. Wählen Sie diese Option aus, um eine Mailbox mit einem der Typen ganz oder teilweise in die ursprüngliche Archivmailbox oder in eine alternative Archivmailbox zurückzuschreiben. Sie können die Archivmailbox filtern und einen bestimmten Mailboxordner zurückschreiben. Geben Sie in das Feld **Zurückzuschreibender Ordner** den Namen des Ordners in der Archivmailbox an, der zurückgeschrieben werden soll. • Um einen Unterordner in einen übergeordneten Ordner zurückzuschreiben, geben Sie den vollständigen Ordnerpfad in diesem Format an: *Name_des_übergeordneten_Ordners/Name_des_Unterordners*. • Um alle Unterordner in einen übergeordneten Ordner zurückzuschreiben, verwenden Sie *Name_des_übergeordneten_Ordners/**. • Wenn der vollständige Ordnerpfad Leerzeichen enthält, schließen Sie den Ordnerpfad in Anführungszeichen ein und hängen Sie keinen umgekehrten Schrägstrich (\) an. Geben Sie im Feld **Zielarchivmailbox** das Archivmailboxziel an.

Tabelle 21. Zurückschreibungsoptionen (Forts.)	
Option	**Aktion**
Wiederherstellbare E-Mail-Einträge beim Zurückschreiben der Mailbox ausschließen	Wenden Sie diese Option an, wenn Sie einen öffentlichen Onlineordner oder eine Archivmailbox in die ursprüngliche Mailbox, in eine alternative Mailbox oder in eine Unicode-PST-Datei zurückzuschreiben. Geben Sie den Wert **Ja** an, um die E-Mail-Einträge im Ordner `Wiederherstellbare Elemente` bei Mailboxzurückschreibungsoperationen auszuschließen. **Nein** ist der Standardwert.

Tipp: Sie können MMC (Microsoft Management Console) aktivieren, um Diagnoseinformationen zu sammeln, die Sie bei der Bestimmung von Problemen mit Zurückschreibungsoperationen unterstützen. Im Rahmen des Prozesses werden Konfigurationsdateien, Tracedateien und allgemeine Diagnoseinformationen der MMC-GUI gesammelt. Weitere Informationen finden Sie in der folgenden Technote: Enabling diagnostic information in the IBM Spectrum Protect Plus MMC GUI(http://www.ibm.com/support/docview.wss?uid=ibm10882270).

17. Wenn die Mailboxzurückschreibungsoperation beendet ist, kehren Sie zu IBM Spectrum Protect Plus zurück. Klicken Sie im Fenster **Jobs und Operationen** > **Aktive Ressourcen** auf **Aktionen** > **Differenzierte Zurückschreibung abbrechen**, um den Prozess der differenzierten Zurückschreibung zu beenden.

DAG-Sicherungen zurückschreiben

Mit IBM Spectrum Protect Plus können Sie die Sicherung einer Exchange Server-Datenbankverfügbarkeitsgruppe (DAG) in die ursprüngliche Instanz oder in eine alternative Instanz zurückschreiben.

Informationen zu diesem Vorgang

In einer DAG-Umgebung müssen Sie eine Datenbank in eine aktive Datenbankkopie zurückschreiben. Wenn Sie eine passive Datenbankkopie als bevorzugtes Ziel von Sicherungsoperationen ausgewählt haben, versucht IBM Spectrum Protect Plus standardmäßig, die Datenbank in diese passive Kopie zurückzuschreiben. Die Zurückschreibungsoperation schlägt fehl. In dieser Situation können Sie auswählen, dass die Datenbank in eine alternative Instanz zurückgeschrieben werden soll, und dann die aktive Datenbankkopie auswählen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Exchange-Zurückschreibungsjob zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Exchange** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch öffnen, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **Exchange** klicken.
   - Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Informationssymbol im Navigationsfenster des Assistenten.
   - Um die optionalen Seiten im Assistenten zu übergehen, wählen Sie **Optionale Schritte überspringen** aus.

2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Schritte aus:

   a) Klicken Sie auf das Menü **Sicht** und wählen Sie **Datenbankverfügbarkeitsgruppen** aus.

   b) Klicken Sie in der Liste **Verfügbarkeitsgruppen** auf eine Exchange-Instanz, um die Liste der Zurückschreibungspunkte für diese Instanz anzuzeigen, und wählen Sie die Sicherungsversionen aus, die zurückgeschrieben werden sollen. Sie können auch die Suchfunktion verwenden, um nach ver-

fügbaren Instanzen zu suchen, und mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen wechseln.

c) Klicken Sie auf das Symbol neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll. Sie können mehrere Datenbanken aus der Liste auswählen.

Die ausgewählten Quellen werden der Zurückschreibungsliste neben der Datenbankliste hinzugefügt. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Symbol neben dem Eintrag.

d) Klicken Sie auf **Weiter**, um fortzufahren.

3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der Datenbank an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren.

Option	Beschreibung
Zurückschreibungstyp	Wählen Sie den Typ des Zurückschreibungsjobs aus: **Bedarfsgesteuert: Momentaufnahme** Führt einen einmaligen Zurückschreibungsjob aus einer Datenbankmomentaufnahme aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Bedarfsgesteuert: Zeitpunkt** Führt einen einmaligen Zurückschreibungsjob aus einer Sicherung einer Datenbank nach Zeitpunkt aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Wiederholt auftretend** Erstellt einen sich wiederholenden Job für die Zurückschreibung nach Zeitpunkt, der gemäß einem Zeitplan ausgeführt wird.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position aus, von der Daten zurückgeschrieben werden sollen: **Site** Die Site, an der Momentaufnahmen gesichert wurden. Die Site wird im Fenster **Systemkonfiguration** > **Site** definiert. **Cloudauslagerung** Der Cloud-Server, auf den Momentaufnahmen ausgelagert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Auslagerung** Der Repository-Server, auf den Momentaufnahmen ausgelagert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert. **Cloudarchivierung** Der Cloud-Server, auf dem Momentaufnahmen archiviert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Archivierung** Der Repository-Server, auf dem Momentaufnahmen archiviert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus: **Demo** Die Demonstrationssite, von der Momentaufnahmen zurückgeschrieben werden sollen.

Option	Beschreibung
	Primär Die primäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. **Sekundär** Die sekundäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, wählen Sie einen Server im Menü **Position auswählen** aus.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datenbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wenn Sie Daten aus einer Cloudressource oder von einem Repository-Server zurückschreiben, wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben; wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert oder in einer Cloudressource oder auf einem Repository-Server archiviert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway auswählen.

4. Geben Sie auf der Seite **Ziel definieren** an, wohin die Datenbank zurückgeschrieben werden soll, und klicken Sie auf **Weiter**.

   In ursprüngliche Instanz zurückschreiben
   Wählen Sie diese Option aus, um die Datenbank auf den ursprünglichen Server zurückzuschreiben.

   In alternative Instanz zurückschreiben
   Wählen Sie diese Option aus, um die Datenbank an ein lokales Ziel zurückzuschreiben, das nicht mit dem ursprünglichen Server übereinstimmt; wählen Sie dann die alternative Position aus der Liste der verfügbaren Server aus.

   Achtung: Wenn Sie das Ziel auswählen, müssen Sie einen aktiven Knoten als Ziel auswählen; andernfalls schlägt die Zurückschreibungsoperation fehl.

5. Wählen Sie auf der Seite **Zurückschreibungsmethode** eine der folgenden Optionen aus:

   - **Test**. Wählen Sie diese Option aus, um die Daten direkt aus dem vSnap-Repository zurückzuschreiben. Dieser Zurückschreibungstyp kann für Testzwecke verwendet werden.
   - **Produktion**. Wählen Sie diese Option aus, um die vollständige Datenbank mit einer Datenzurückschreibungsoperation anhand einer vollständigen Kopie zurückzuschreiben. Diese Zurückschreibungsoperation ist für die permanente Verwendung der zurückgeschriebenen Datenbank bestimmt.

   Klicken Sie auf **Weiter**, um fortzufahren.

6. Optional: Konfigurieren Sie auf der Seite **Joboptionen** weitere Optionen für den Zurückschreibungsjob und klicken Sie auf **Weiter**, um fortzufahren.

   Wiederherstellungsoptionen
   Wählen Sie eine der folgenden Wiederherstellungsoptionen aus:

Keine Wiederherstellung
Mit dieser Option wird jede aktualisierende Wiederherstellung nach der Zurückschreibungsoperation übersprungen. Die Datenbank verbleibt in einem Status `Aktualisierende Wiederherstellung anstehend`, bis Sie entscheiden, ob die aktualisierende Wiederherstellung manuell ausgeführt werden soll.

Bis zum Ende der Sicherung wiederherstellen
Mit dieser Option wird die ausgewählte Datenbank mit dem Status zum Zeitpunkt der Erstellung der Sicherung zurückgeschrieben.

Bis zum Ende der verfügbaren Protokolle wiederherstellen
Mit dieser Option wird die Datenbank zurückgeschrieben und alle verfügbaren Protokolle (einschließlich der Protokolle, die neuer als die Sicherung sind, die möglicherweise auf dem Anwendungsserver vorhanden ist) werden angewendet, um die Datenbank mit dem Stand des letztmöglichen Zeitpunkts wiederherzustellen. Diese Option ist nur verfügbar, wenn Sie **Protokollsicherung aktivieren** im Sicherungsjob ausgewählt haben.

Bis zu einem bestimmten Zeitpunkt wiederherstellen
Wenn Protokollsicherungen aktiviert sind, wird mit dieser Option die Datenbank zurückgeschrieben und Protokolle vom Protokollsicherungsdatenträger werden angewendet, um die Datenbank bis zu einem benutzerdefinierten Zwischenzeitpunkt wiederherzustellen. Wählen Sie das Datum und die Uhrzeit über die Optionen für **Nach Zeit** aus.

Anwendungsoptionen
Definieren Sie die Anwendungsoptionen:

Maximale Anzahl paralleler Datenströme pro Datenbank
Definieren Sie die maximale Anzahl Datenströme pro Datenbank aus dem Sicherungsspeicher. Diese Einstellung gilt für jede Datenbank in der Jobdefinition. Mehrere Datenbanken können auch dann parallel zurückgeschrieben werden, wenn der Wert der Option auf 1 gesetzt wird. Mehrere parallele Datenströme können die Zurückschreibungsgeschwindigkeit verbessern, die Nutzung hoher Bandbreite kann sich jedoch auf die Systemgesamtleistung auswirken.

Diese Option ist nur gültig, wenn Sie eine Exchange-Datenbank mit ihrem ursprünglichen Datenbanknamen an die ursprüngliche Position zurückschreiben.

Erweiterte Optionen
Definieren Sie die erweiterten Jobdefinitionsoptionen:

Bereinigung direkt beim Fehlschlagen des Jobs ausführen
Aktivieren Sie diese Option, um zugeordnete Ressourcen automatisch im Rahmen einer Zurückschreibung zu bereinigen, wenn die Wiederherstellung fehlschlägt.

7. Optional: Wählen Sie auf der Seite **Scripts anwenden** das anzuwendende **Vorscript** oder **Nachscript** aus oder wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus. Weitere Informationen zum Arbeiten mit Scripts finden Sie in Scripts konfigurieren. Klicken Sie auf **Weiter**, um fortzufahren.
8. Führen Sie auf der Seite **Zeitplan** eine der folgenden Aktionen aus:
   - Wenn Sie einen bedarfsgesteuerten Job ausführen, klicken Sie auf **Weiter**.
   - Wenn Sie einen sich wiederholenden Job definieren, geben Sie einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an. Klicken Sie auf **Weiter**.
9. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs und klicken Sie auf **Übergeben**, um den Job zu erstellen.

   Der Zurückschreibungsjob wird erstellt; Sie können seinen Status über **Jobs und Operationen** > **Aktive Jobs** überprüfen.

Im Instant Access-Modus auf Exchange-Datenbankdateien zugreifen

Mithilfe des Zurückschreibungstyps "Instant Access" können Sie auf die Microsoft Exchange-Datenbankdateien zugreifen und die Datenbankdateien auf dem vSnap-Datenträger einem Anwendungsserver bereitstellen.

Informationen zu diesem Vorgang
Im Instant Access-Modus wird keine weitere Aktion ausgeführt, nachdem IBM Spectrum Protect Plus die Freigabe bereitgestellt hat. Verwenden Sie die Daten für die angepasste Wiederherstellung von Daten aus den Dateien auf dem vSnap-Datenträger.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Exchange** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch öffnen, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **Exchange** klicken.
   - Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Informationssymbol im Navigationsfenster des Assistenten.
   - Um die optionalen Seiten im Assistenten zu übergehen, wählen Sie **Optionale Schritte überspringen** aus.
2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Schritte aus:
   a) Klicken Sie in der Liste auf eine Quelle, um die Datenbanken anzuzeigen, die für Zurückschreibungsoperationen verfügbar sind. Sie können auch die Suchfunktion verwenden, um nach verfügbaren Instanzen zu suchen, und mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen wechseln.

   b) Klicken Sie auf das Plussymbol neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll. Sie können mehrere Datenbanken aus der Liste auswählen.

   Die ausgewählten Quellen werden der Zurückschreibungsliste neben der Datenbankliste hinzugefügt. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Minussymbol neben dem Eintrag.

   c) Klicken Sie auf **Weiter**, um fortzufahren.
3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der Datenbank an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren.

Option	Beschreibung
Zurückschreibungstyp	Wählen Sie den Typ des Zurückschreibungsjobs aus: **Bedarfsgesteuert: Momentaufnahme** Führt einen einmaligen Zurückschreibungsjob aus einer Datenbankmomentaufnahme aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Bedarfsgesteuert: Zeitpunkt** Führt einen einmaligen Zurückschreibungsjob aus einer Sicherung einer Datenbank nach Zeitpunkt aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Wiederholt auftretend** Erstellt einen sich wiederholenden Job für die Zurückschreibung nach Zeitpunkt, der gemäß einem Zeitplan ausgeführt wird.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position aus, von der Daten zurückgeschrieben werden sollen: **Site** Die Site, an der Momentaufnahmen gesichert wurden. Die Site wird im Fenster **Systemkonfiguration** > **Site** definiert.

Option	Beschreibung
	Cloudauslagerung Der Cloud-Server, auf den Momentaufnahmen ausgelagert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Auslagerung** Der Repository-Server, auf den Momentaufnahmen ausgelagert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert. **Cloudarchivierung** Der Cloud-Server, auf dem Momentaufnahmen archiviert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Archivierung** Der Repository-Server, auf dem Momentaufnahmen archiviert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus: **Demo** Die Demonstrationssite, von der Momentaufnahmen zurückgeschrieben werden sollen. **Primär** Die primäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. **Sekundär** Die sekundäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, wählen Sie einen Server im Menü **Position auswählen** aus.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datenbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wenn Sie Daten aus einer Cloudressource oder von einem Repository-Server zurückschreiben, wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben; wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert oder in einer Cloudressource oder auf einem Repository-Server archiviert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway auswählen.

4. Geben Sie auf der Seite **Ziel definieren** an, wo die Datenbankdateien bereitgestellt werden sollen, und klicken Sie auf **Weiter**.

Option	Beschreibung
An ursprüngliche Position zurückschreiben	Wählen Sie diese Option aus, um die Datenbankdateien auf dem ursprünglichen Server bereitzustellen.
An alternative Position zurückschreiben	Wählen Sie diese Option aus, um die Datenbankdateien an einem lokalen Ziel bereitzustellen, das nicht mit dem ursprünglichen Server übereinstimmt; wählen Sie dann die alternative Position aus der Liste der verfügbaren Server aus.

5. Wählen Sie auf der Seite **Zurückschreibungsmethode Instant Access** aus und klicken Sie dann auf **Weiter**.
6. Optional: Konfigurieren Sie auf der Seite **Joboptionen**, falls erforderlich, weitere Optionen und klicken Sie auf **Weiter**, um fortzufahren.
7. Optional: Wählen Sie auf der Seite **Scripts anwenden** das anzuwendende **Vorscript** oder **Nachscript** aus oder wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus. Weitere Informationen zum Arbeiten mit Scripts finden Sie in Scripts konfigurieren. Klicken Sie auf **Weiter**, um fortzufahren.
8. Führen Sie auf der Seite **Zeitplan** eine der folgenden Aktionen aus:
   - Wenn Sie einen bedarfsgesteuerten Job ausführen, klicken Sie auf **Weiter**.
   - Wenn Sie einen sich wiederholenden Job definieren, geben Sie einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an. Klicken Sie auf **Weiter**.
9. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs und klicken Sie auf **Übergeben**, um den Job zu erstellen.

   Der Zurückschreibungsjob wird erstellt; Sie können seinen Status über **Jobs und Operationen** > **Aktive Jobs** überprüfen.
10. Sie können jetzt auf die Exchange-Datenbankdateien am Mountpunkt des Anwendungsservers zugreifen und jede gewünschte Exchange-bezogene oder angepasste Aktion ausführen.

    Anmerkung: Die Exchange-Datenbankdateien am Mountpunkt sind im Schreib-/Lesezugriff. Durch ihre Aktualisierung wird die ursprüngliche Sicherung jedoch nicht geändert.
11. Wenn die Instant Access-Zurückschreibungsoperation abgeschlossen ist, rufen Sie das Fenster **Aktive Ressourcen** auf und klicken Sie auf **Aktionen** > **Zurückschreibung abbrechen**, um die bereitgestellte Datenbank zu entfernen und den Zurückschreibungsprozess zu beenden.

MongoDB

Nachdem Sie MongoDB-Instanzen in IBM Spectrum Protect Plus erfolgreich hinzugefügt haben, ist der Schutz der Daten in Ihren MongoDB-Datenbanken möglich. Erstellen Sie SLA-Richtlinien (SLA = Service-Level-Agreement) zur Sicherung und Verwaltung von MongoDB-Daten.

Stellen Sie sicher, dass Ihre MongoDB-Umgebung die Systemanforderungen erfüllt. Weitere Informationen finden Sie in „MongoDB-Anforderungen” auf Seite 34.

Voraussetzungen für MongoDB

Alle Systemanforderungen und -voraussetzungen für den IBM Spectrum Protect Plus MongoDB-Anwendungsserver müssen erfüllt sein, bevor Sie MongoDB-Daten mit IBM Spectrum Protect Plus schützen.

Informationen zu MongoDB-Systemanforderungen finden Sie in MongoDB-Anforderungen.

Um die Voraussetzungen für MongoDB zu erfüllen, führen Sie die folgenden Prüfungen und Aktionen aus.

1. Stellen Sie sicher, dass die in Speichervoraussetzungen für MongoDB-Schutz beschriebenen Speichervoraussetzungen erfüllt sind.
2. Setzen Sie die Dateigrößenbegrenzung für den MongoDB-Instanzbenutzer mit dem Befehl **`ulimit`** -f auf "unlimited". Es ist auch möglich, den Wert auf einen ausreichend hohen Wert zu setzen, der das

Kopieren der größten Datenbankdateien in Ihren Sicherungs- und Zurückschreibungsjobs ermöglicht. Wenn Sie die Einstellung für **ulimit** ändern, starten Sie die MongoDB-Instanz erneut, um die Konfiguration abzuschließen.

3. Wenn Sie MongoDB in einer AIX- oder Linux-Umgebung ausführen, stellen Sie sicher, dass die installierte sudo-Version einen unterstützten Stand hat.

   Weitere Informationen zum Versionsstand finden Sie in „MongoDB-Anforderungen" auf Seite 34. Informationen zum Festlegen von sudo-Berechtigungen finden Sie in „Sudo-Berechtigungen definieren" auf Seite 208.
4. Wenn Ihre MongoDB-Datenbanken durch Authentifizierung geschützt werden, müssen Sie die rollenbasierte Zugriffssteuerung definieren. Weitere Informationen finden Sie in „Rollen für MongoDB" auf Seite 206.
5. Jede MongoDB-Instanz, die geschützt werden soll, muss in IBM Spectrum Protect Plus registriert werden. Nachdem die Instanzen registriert wurden, führt IBM Spectrum Protect Plus eine Bestandsoperation aus, um MongoDB-Ressourcen zu erkennen. Stellen Sie sicher, dass alle Instanzen, die geschützt werden sollen, erkannt und korrekt aufgelistet werden.
6. Stellen Sie sicher, dass der SSH-Service an Port 22 auf dem Server aktiv ist und Firewalls so konfiguriert sind, dass sie IBM Spectrum Protect Plus das Herstellen der Verbindung zum Server mit SSH ermöglichen. Das Subsystem SFTP für SSH muss aktiviert sein.
7. Stellen Sie sicher, dass keine verschachtelten Mountpunkte konfiguriert werden.

Einschränkungen

Die folgenden Einschränkungen gelten für den MongoDB-Anwendungsserver:

- Sharded MongoDB-Clusterkonfigurationen werden erkannt, wenn Sie eine Bestandsoperation ausführen; diese Ressourcen sind jedoch nicht für Sicherungs- oder Zurückschreibungsoperationen auswählbar.
- Unicode-Zeichen in MongoDB-Dateipfadnamen können nicht von IBM Spectrum Protect Plus verarbeitet werden. Alle Namen müssen in ASCII codiert sein.

Virtualisierung

Schützen Sie Ihre MongoDB-Umgebung mit IBM Spectrum Protect Plus, wenn sie auf einem der folgenden Gastbetriebssysteme ausgeführt wird:

- Red Hat Enterprise Linux
- KVM (kernelbasierte virtuelle Maschine) unter SUSE Linux Enterprise Server

Rollen für MongoDB

Sie müssen RBAC-Rollen für die MongoDB-Agentenbenutzer definieren, wenn die Authentifizierung in der MongoDB-Datenbank aktiviert ist. Beim Definieren der Rollen können Benutzer MongoDB-Ressourcen mit IBM Spectrum Protect Plus in Übereinstimmung mit den für die Benutzer definierten Rollen schützen und überwachen.

Rollenbasierte Zugriffssteuerung für MongoDB

Geben Sie für jeden MongoDB-Benutzer unter Verwendung eines ähnlichen Befehls wie in dem folgenden Beispiel Zugriffsrollen an:

```
use admin
db.grantRolesToUser("<Benutzername>",
[ { role: "hostManager", db: "admin" },
{ role: "clusterManager", db: "admin" } ] )
```

Die folgenden Rollen sind verfügbar:

hostManager
Diese Rolle stellt Zugriff auf den Befehl **fsyncLock** bereit. Dieser Zugriff ist für anwendungskonsistente Sicherungen von MongoDB-Datenbanken erforderlich, bei denen Journaling nicht aktiviert ist. Diese Rolle stellt außerdem Zugriff auf den Befehl "shutdown" bereit, der während einer Zurückschreibungsoperation zum Herunterfahren der MongoDB-Serverinstanz verwendet wird, die das Ziel der Zurückschreibung ist.

clusterMonitor
Diese Rolle stellt Zugriff auf Befehle zum Überwachen und Lesen des Status der MongoDB-Datenbank bereit. Für Benutzer mit dieser Rolle sind die folgenden Befehle verfügbar:

- **getCmdLineOpts**
- **serverVersion**
- **replSetGetConfig**
- **replSetGetStatus**
- **isMaster**
- **listShards**

clusterManager
Diese Rolle ist nur zur Ausführung von Testzurückschreibungsoperationen für Replikatgruppen erforderlich. Benutzer, die den Befehl **replSetReconfig** ausführen, können die zurückgeschriebene Instanz einer Einzelknotenreplikatgruppe erstellen. Diese Rolle ermöglicht den Schreib-/Lesezugriff während Testzurückschreibungsoperationen für Replikatgruppen. Ohne diesen Zugriff würde der Knoten in der Replikatgruppe ohne Schreib-/Lesezugriff im Status REMOVED verbleiben. Darüber hinaus stellt diese Rolle Zugriff auf Befehle zum Lesen des Status der MongoDB-Datenbank bereit. Für diese Rolle sind die folgenden Befehle verfügbar:

- **replSetReconfig**
- **getCmdLineOpts**
- **serverVersion**
- **replSetGetConfig**
- **replSetGetStatus**
- **isMaster**
- **listShards**

Speichervoraussetzungen für MongoDB-Schutz
Bevor Sie MongoDB-Daten sichern, müssen Sie sicherstellen, dass genügend freier Speicherbereich auf den Ziel- und Quellenhosts und im vSnap-Repository vorhanden ist. Zusätzlicher Speicherbereich ist erforderlich, um temporäre LVM-Sicherungen logischer Datenträger, auf denen sich die MongoDB-Daten befinden, speichern zu können. Diese temporären Sicherungen, die als LVM-Momentaufnahmen bezeichnet werden, werden automatisch vom MongoDB-Agenten erstellt.

LVM-Momentaufnahmen

LVM-Momentaufnahmen sind Zeitpunktkopien logischer LVM-Datenträger. Nachdem die Dateikopieroperation beendet ist, werden frühere LVM-Momentaufnahmen vom IBM Spectrum Protect Plus MongoDB-Agenten in einer Bereinigungsoperation entfernt.

Für jeden logischen LVM-Momentaufnahmedatenträger müssen Sie mindestens 10 Prozent freien Speicherbereich in der Datenträgergruppe reservieren. Wenn in der Datenträgergruppe genügend freier Speicherbereich vorhanden ist, reserviert der IBM Spectrum Protect Plus MongoDB-Agent bis zu 25 Prozent der Größe des logischen Quellendatenträgers für den logischen Momentaufnahmedatenträger.

Linux-LVM2
Wenn Sie eine MongoDB-Sicherungsoperation ausführen, fordert MongoDB eine Momentaufnahme an. Diese Momentaufnahme wird auf einem Logical Volume Manager-System (LVM-System) für jeden logi-

schen Datenträger mit Daten oder Protokollen für die ausgewählte Datenbank erstellt. Auf Linux-Systemen werden logische Datenträger von LVM2 verwaltet.

Eine softwarebasierte LVM2-Momentaufnahme wird als neuer logischer Datenträger in derselben Datenträgergruppe erstellt. Die Momentaufnahmedatenträger werden vorübergehend auf derselben Maschine bereitgestellt, die die MongoDB-Instanz ausführt, sodass sie in das vSnap-Repository übertragen werden können.

Unter Linux speichert der LVM2-Datenträgermanager die Momentaufnahme eines logischen Datenträgers in derselben Datenträgergruppe. Es muss genügend Speicherbereich zum Speichern des logischen Datenträgers verfügbar sein. Die Größe des logischen Datenträgers nimmt in dem Maße zu, wie sich die Daten auf dem Quellendatenträger für die Lebensdauer der Momentaufnahme ändern.

Sudo-Berechtigungen definieren

Um IBM Spectrum Protect Plus zum Schützen Ihrer Daten zu verwenden, müssen Sie die erforderliche Version des sudo-Programms installieren.

Informationen zu diesem Vorgang

Definieren Sie einen dedizierten IBM Spectrum Protect Plus-Agentenbenutzer mit den erforderlichen Superuserberechtigungen für sudo. Diese Konfiguration ermöglicht es Agentenbenutzern, Befehle ohne ein Kennwort auszuführen.

Vorgehensweise

1. Erstellen Sie einen Agentenbenutzer, indem Sie den folgenden Befehl ausgeben:

   `useradd -m` *`Agent`*

   Dabei gibt *Agent* den Namen des IBM Spectrum Protect Plus-Agentenbenutzers an.
2. Definieren Sie ein Kennwort für den neuen Benutzer, indem Sie den folgenden Befehl ausgeben:

   `passwd` *`MongoDB-Agent`*
3. Um Superuserberechtigungen für den Agentenbenutzer zu aktivieren, definieren Sie die Einstellung `!requiretty`. Fügen Sie am Ende der sudo-Konfigurationsdatei die folgenden Zeilen hinzu:

   ```
   Defaults:Agent !requiretty
   Agent ALL=(ALL) NOPASSWD:ALL
   ```

   Wenn Ihre sudoers-Datei für den Import von Konfigurationen aus einem anderen Verzeichnis (beispielsweise `/etc/sudoers.d`) konfiguriert ist, können Sie die Zeilen auch in der entsprechenden Datei in diesem Verzeichnis hinzufügen.

MongoDB-Anwendungsserver hinzufügen

Um MongoDB-Ressourcen zu schützen, müssen Sie zunächst den Server hinzufügen, auf dem sich Ihre MongoDB-Instanzen befinden, und Berechtigungsnachweise für die Instanzen definieren. Wiederholen Sie die Prozedur, um alle Server hinzuzufügen, auf denen sich MongoDB-Ressourcen befinden.

Informationen zu diesem Vorgang

Um IBM Spectrum Protect Plus einen MongoDB-Anwendungsserver hinzuzufügen, müssen Sie über die Hostadresse der Maschine verfügen.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **MongoDB**.
2. Klicken Sie im Fenster **MongoDB** auf **Anwendungsserver verwalten** und klicken Sie auf **Anwendungsserver hinzufügen**, um die Hostmaschine hinzuzufügen.

3. Geben Sie in der Maske **Anwendungseigenschaften** die Hostadresse ein.
4. Wählen Sie aus, ob der Host mit einem Benutzer oder einem SSH-Schlüssel registriert werden soll.

   Wenn Sie **Benutzer** auswählen, können Sie einen neuen Benutzer und ein neues Kennwort oder einen vorhandenen Benutzer eingeben. Wenn Sie **SSH-Schlüssel** auswählen, wählen Sie den SSH-Schlüssel aus dem Menü aus.

   Einschränkung: Für jeden angegebenen Benutzer müssen sudo-Berechtigungen definiert werden.

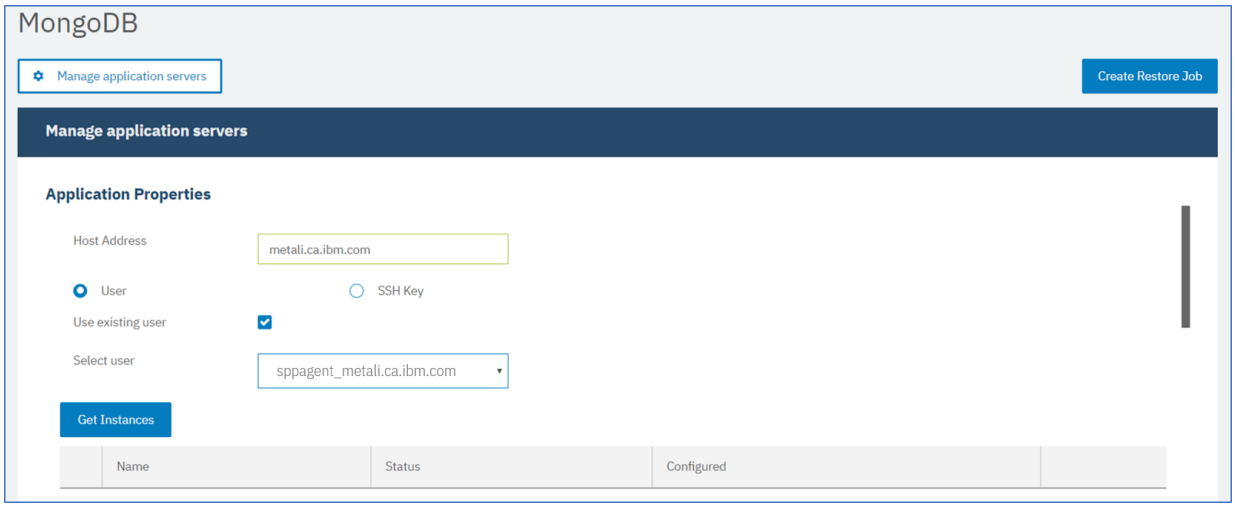


Abbildung 25. MongoDB-Agent hinzufügen

5. Klicken Sie auf **Instanzen abrufen**, um die MongoDB-Instanzen zu erkennen und aufzulisten, die auf dem Host-Server verfügbar sind, der hinzugefügt wird.

   Jede MongoDB-Instanz wird mit der Hostadresse der Verbindung, dem Status und einer Angabe aufgelistet, ob sie konfiguriert ist.

   Achtung: Wenn Sie mehr als einen Anwendungsserver für eine einzige Replikatgruppe registrieren, kann sich der angezeigte Instanzname nach jeder Bestands-, Sicherungs- oder Zurückschreibungsoperation ändern. Der Hostname des zuletzt hinzugefügten Anwendungsservers, der zu der Replikatgruppe gehört, wird als Teil des Instanznamens verwendet. Eine Bestandsoperation wird als Teil von Sicherungs- und Zurückschreibungsoperationen ausgeführt.
6. Wenn Sie die Zugriffssteuerung verwenden, konfigurieren Sie eine Instanz, indem Sie Berechtigungsnachweise definieren. Klicken Sie auf **Berechtigungsnachweis definieren** und definieren Sie die Benutzer-ID und das Kennwort. Alternativ können Sie ein vorhandenes Benutzerprofil verwenden.

   Weitere Informationen zur Zugriffssteuerung finden Sie in Kapitel 13, „Benutzerzugriff verwalten", auf Seite 311.

   Wenn Sie Berechtigungsnachweise definieren, ordnen Sie MongoDB-Benutzerrollen für die Sicherungs- und Zurückschreibungsoperationen mit Zugriff auf rollengeschützte MongoDB-Server zu, indem Sie das SCRAM-Authentifizierungsverfahren (SCRAM = Salted Challenge Response Authentication Mechanism) oder die Challenge-Response-Authentifizierung verwenden. Der MongoDB-Benutzer, der für den rollengeschützten MongoDB-Server zugeordnet wird, erfordert eine der folgenden Zugriffsebenen, um Ressourcen zu schützen:

   - *hostManager*: Verwaltet die Datenbank als Administrator. Diese Rolle ist für die Erstellung und Verwaltung von Momentaufnahmen erforderlich.
   - *clusterAdmin*: Ruft Konfigurationsinformationen ab und führt Zurückschreibungsoperationen im Testmodus für MongoDB-Replikatgruppen aus. Diese Rolle ist erforderlich, um Zurückschreibungsoperationen im Testmodus für MongoDB-Replikatgruppen für Datenabfragen zu rekonfigurieren.
   - *clusterMonitor*: Überwacht den Schutz von MongoDB-Ressourcen und ruft Konfigurationsinformationen ab.

7. Optional: Definieren Sie die Option **Maximale Anzahl gleichzeitig verwendeter Datenbanken**, indem Sie eine Zahl in das Feld eingeben.
8. Speichern Sie die Maske und wiederholen Sie die Schritte, um IBM Spectrum Protect Plus weitere MongoDB-Anwendungsserver hinzuzufügen.

Nächste Schritte

Nachdem Sie IBM Spectrum Protect Plus Ihre MongoDB-Anwendungsserver hinzugefügt haben, wird automatisch auf jedem Anwendungsserver eine Bestandsverarbeitung ausgeführt, um die relevanten Datenbanken in diesen Instanzen zu erkennen.

Um zu verifizieren, ob die Datenbanken hinzugefügt wurden, überprüfen Sie das Jobprotokoll. Rufen Sie **Jobs und Operationen** auf. Klicken Sie auf die Registerkarte **Aktive Jobs** und suchen Sie nach dem neuesten Bestandsprotokolleintrag für den Anwendungsserver.

Beendete Jobs werden auf der Registerkarte **Jobprotokoll** angezeigt. Mithilfe der Liste **Sortieren nach** können Sie Jobs auf der Basis von Startzeit, Typ, Status, Jobnamen oder Dauer sortieren. Verwenden Sie das Feld **Nach Namen suchen**, um nach Jobs anhand des Namens zu suchen. Sie können Sterne als Platzhalterzeichen in dem Namen verwenden.

Datenbanken müssen erkannt werden, damit sie geschützt werden können. Anweisungen zur Ausführung einer manuellen Bestandsverarbeitung finden Sie in MongoDB-Ressourcen erkennen.

MongoDB-Ressourcen erkennen

Nachdem Sie IBM Spectrum Protect Plus Ihre MongoDB-Anwendungsserver hinzugefügt haben, wird automatisch eine Bestandsverarbeitung ausgeführt, um alle MongoDB-Instanzen und -Datenbanken zu erkennen. Sie können eine manuelle Bestandsverarbeitung auf jedem Anwendungsserver ausführen, um alle MongoDB-Datenbanken für den ausgewählten Host zu erkennen, aufzulisten und zu speichern.

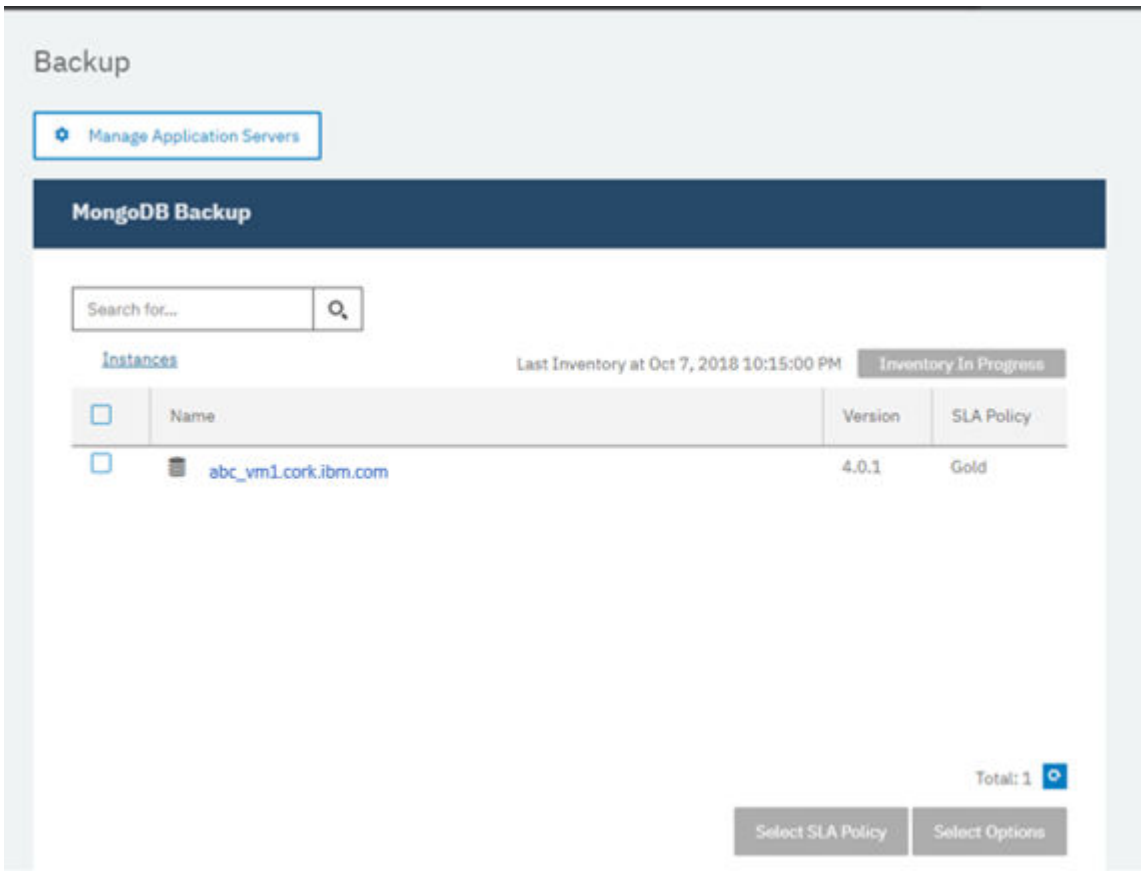
Vorbereitende Schritte

Stellen Sie sicher, dass Sie IBM Spectrum Protect Plus Ihre MongoDB-Anwendungsserver hinzugefügt haben. Anweisungen finden Sie in MongoDB-Anwendungsserver hinzufügen.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **MongoDB**.

   Tipp: Um dem Fenster **Instanzen** weitere MongoDB-Instanzen hinzuzufügen, führen Sie die Anweisungen in MongoDB-Anwendungsserver hinzufügen aus.
2. Klicken Sie auf **Bestandsverarbeitung ausführen**.



Bei der Ausführung der Bestandsverarbeitung ändert sich die Schaltfläche in **Bestandsverarbeitung wird ausgeführt**. Sie können eine Bestandsverarbeitung auf allen verfügbaren Anwendungsservern ausführen, Sie können jedoch nur jeweils einen einzigen Bestandsprozess ausführen.

Um den Bestandsjob zu überwachen, rufen Sie **Jobs und Operationen** auf. Klicken Sie auf die Registerkarte **Aktive Jobs** und suchen Sie nach dem neuesten Bestandsprotokolleintrag für den Anwendungsserver.

Beendete Jobs werden auf der Registerkarte **Jobprotokoll** angezeigt. Mithilfe der Liste **Sortieren nach** können Sie Jobs auf der Basis von Startzeit, Typ, Status, Jobnamen oder Dauer sortieren. Verwenden Sie das Feld **Nach Namen suchen**, um nach Jobs anhand des Namens zu suchen. Sie können Sterne als Platzhalterzeichen in dem Namen verwenden.

3. Klicken Sie auf eine Instanz, um eine Sicht zu öffnen, in der die für diese Instanz erkannten Datenbanken angezeigt werden. Wenn Datenbanken in der Liste **Instanzen** fehlen, überprüfen Sie Ihren MongoDB-Anwendungsserver und führen Sie den Bestandsjob erneut aus. In einigen Fällen sind bestimmte Datenbanken als nicht auswählbar für die Sicherung markiert; bewegen Sie den Mauszeiger über die Datenbank, um den Grund sichtbar zu machen.

Tipp: Um zur Liste der Instanzen zurückzukehren, klicken Sie auf den Link **Instanzen** im Fenster **MongoDB-Sicherung**.

Achtung: Wenn Sie mehr als einen Anwendungsserver für eine einzige Replikatgruppe registrieren, kann sich der angezeigte Instanzname nach jeder Bestands-, Sicherungs- oder Zurückschreibungsoperation ändern. Der Hostname des zuletzt dem Bestand hinzugefügten Anwendungsservers, der zu der Replikatgruppe gehört, wird als Teil des Instanznamens verwendet. Eine Bestandsoperation wird als Teil von Sicherungs- und Zurückschreibungsoperationen ausgeführt.

Nächste Schritte

Um die MongoDB-Datenbanken zu schützen, die in der ausgewählten Instanz katalogisiert sind, wenden Sie eine SLA-Richtlinie (SLA = Service-Level-Agreement) auf die Instanz an. Anweisungen zum Definieren einer SLA-Richtlinie finden Sie in SLA-Richtlinie definieren.

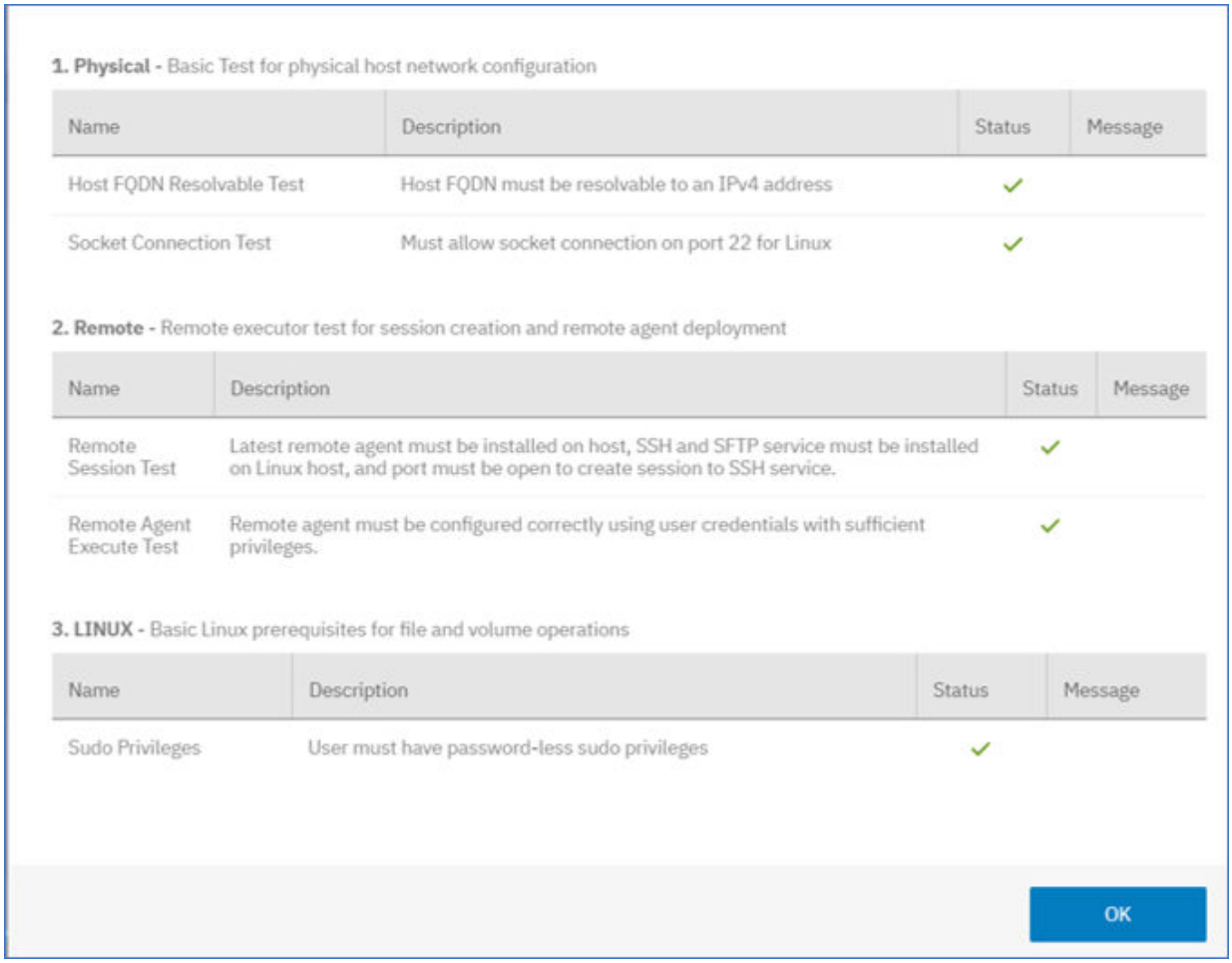
MongoDB-Verbindung testen

Nachdem Sie einen MongoDB-Anwendungsserver hinzugefügt haben, können Sie die Verbindung testen. Bei dem Test wird die Kommunikation zwischen IBM Spectrum Protect Plus und dem MongoDB-Server verifiziert. Außerdem wird überprüft, ob die korrekten sudo-Berechtigungen für den Benutzer verfügbar sind, der den Test ausführt.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **MongoDB**.
2. Klicken Sie im Fenster **MongoDB** auf **Anwendungsserver verwalten** und wählen Sie die Hostadresse aus, die getestet werden soll.

   Eine Liste der verfügbaren MongoDB-Anwendungsserver wird angezeigt.
3. Klicken Sie auf **Aktionen** und wählen Sie **Testen** aus, um die Prüftests für physische Verbindungen und Verbindungen zu einem fernen System und Einstellungen zu starten.



   Der Testbericht zeigt eine Liste, die Tests für die Netzkonfiguration des physischen Hosts und Tests für die Installation des fernen Servers auf dem Host einschließt.
4. Klicken Sie auf **OK**, um den Testbericht zu schließen. Werden Probleme zurückgemeldet, beheben Sie die Probleme und führen Sie den Test erneut aus, um die Fixes zu verifizieren.

MongoDB-Daten sichern

Definieren Sie regelmäßige MongoDB-Sicherungsjobs mit Optionen zum Ausführen und Erstellen von Sicherungskopien zum Schutz Ihrer Daten. Um Ihre Daten regelmäßig zu sichern, definieren Sie einen Sicherungsjob, der eine SLA-Richtlinie (SLA = Service-Level-Agreement) einschließt.

Vorbereitende Schritte

Während der Erstsicherung erstellt IBM Spectrum Protect Plus einen neuen vSnap-Datenträger und eine neue NFS-Freigabe. Bei Teilsicherungen wird der zuvor erstellte Datenträger wiederverwendet. Der IBM Spectrum Protect Plus MongoDB-Agent stellt die Freigabe auf dem MongoDB-Server bereit, auf dem die Sicherung ausgeführt wird.

Lesen Sie die folgenden Voraussetzungen, bevor Sie eine Sicherungsjobdefinition erstellen:

- Fügen Sie die Anwendungsserver hinzu, die gesichert werden sollen. Die Prozedur finden Sie in MongoDB-Anwendungsserver hinzufügen.
- Konfigurieren Sie eine SLA-Richtlinie. Die Prozedur finden Sie in SLA-Sicherungsjob definieren.
- Bevor ein IBM Spectrum Protect Plus-Benutzer Sicherungs- und Zurückschreibungsoperationen definieren kann, müssen dem Benutzer Rollen und Ressourcengruppen zugeordnet werden. Erteilen Sie Benutzern mithilfe des Fensters **Accounts** Zugriff auf Ressourcen und Sicherungs- und Zurückschreibungsoperationen. Weitere Informationen finden Sie in Kapitel 13, „Benutzerzugriff verwalten”, auf Seite 311 und „Rollen für MongoDB” auf Seite 206.
- Vermeiden Sie die Konfiguration von Protokollsicherungen für eine einzelne MongoDB-Datenbank mit vielen Sicherungsjobs. Wenn eine einzelne MongoDB-Datenbank mehreren Jobdefinitionen hinzugefügt wird, kann eine Protokollsicherung von einem Job ein Protokoll abschneiden, bevor es vom nächsten Job gesichert wird. Diese Arbeitslast kann zur Folge haben, dass Jobs zum Zurückschreiben nach Zeitpunkt fehlschlagen.
- Die Wiederherstellung nach Zeitpunkt wird nicht unterstützt, wenn eine oder mehrere Datendateien der Datenbank in dem Zeitraum zwischen dem ausgewählten Zeitpunkt und der Zeit hinzugefügt werden, zu der der vorherige Sicherungsjob ausgeführt wurde.

Einschränkung: Führen Sie keine Bestandsjobs aus, wenn zu derselben Zeit Sicherungsjobs geplant sind.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **MongoDB**.
2. Wählen Sie das Kontrollkästchen für die Instanz aus, die gesichert werden soll.

   Unter jeder MongoDB-Instanz werden die zu sichernden Daten als **ALLE** aufgelistet. Jede Instanz im Fenster "Instanzen" wird nach Instanznamen, Version und der angewendeten SLA-Richtlinie aufgelistet.
3. Klicken Sie auf **Optionen auswählen**, um die Anzahl paralleler Datenströme für die Sicherungsoperation anzugeben, und klicken Sie dann auf **Speichern**. Durch die Auswahl einer entsprechenden Anzahl paralleler Datenströme können Sie die Zeit minimieren, die für den Sicherungsjob erforderlich ist.

   Die gespeicherten Optionen werden wie ausgewählt für alle Sicherungsjobs für diese Instanz verwendet.
4. Um den Sicherungsjob mit diesen Optionen auszuführen, klicken Sie auf den Instanznamen, wählen Sie die Datenbankdarstellung **ALLE** aus und klicken Sie auf **Ausführen**.

   Der Sicherungsjob startet und Sie können die Details über **Jobs und Operationen** > **Aktive Jobs** anzeigen.

   Tipp: Die Schaltfläche **Ausführen** ist nur aktiviert, wenn eine SLA-Richtlinie auf die Darstellung **ALLE** der Datenbanken angewendet wird.
5. Wählen Sie die Instanz erneut aus und klicken Sie auf **SLA-Richtlinie auswählen**, um eine SLA-Richtlinie auszuwählen.
6. Speichern Sie die SLA-Auswahl.

Um eine neue SLA-Richtlinie zu definieren oder eine vorhandene Richtlinie mit angepassten Raten für die Aufbewahrung und Häufigkeit zu editieren, wählen Sie **Schutz verwalten** > **Richtlinienübersicht** aus. Klicken Sie im Fenster **SLA-Richtlinien** auf **SLA-Richtlinie hinzufügen** und definieren Sie die Richtlinienvorgaben.

Nächste Schritte

Nachdem die SLA-Richtlinie gespeichert wurde, können Sie die Richtlinie zu jeder Zeit ausführen, indem Sie auf **Aktionen** neben dem Richtliniennamen klicken und **Starten** auswählen. Der Status im Protokoll ändert sich, um anzuzeigen, dass sich der Sicherungsjob im Status `Aktiv` befindet.

Um einen aktiven Job abzubrechen, klicken Sie auf **Aktionen** neben dem Richtliniennamen und wählen Sie **Abbrechen** aus. In einer Nachricht wird gefragt, ob die Daten aufbewahrt werden sollen, die bereits gesichert wurden. Wählen Sie **Ja** aus, um die gesicherten Daten aufzubewahren, oder wählen Sie **Nein** aus, um die Sicherung zu löschen.

Regelmäßigen SLA-Job definieren

Nachdem Ihre MongoDB-Instanzen aufgelistet wurden, wählen Sie eine SLA-Richtlinie aus und wenden Sie die Richtlinie an, um Ihre Daten zu schützen.

Vorgehensweise

1. Erweitern Sie im Navigationsfenster **Schutz verwalten** > **Anwendungen** > **MongoDB**.
2. Wählen Sie die MongoDB-Instanz aus, um alle Daten in dieser Instanz zu sichern.

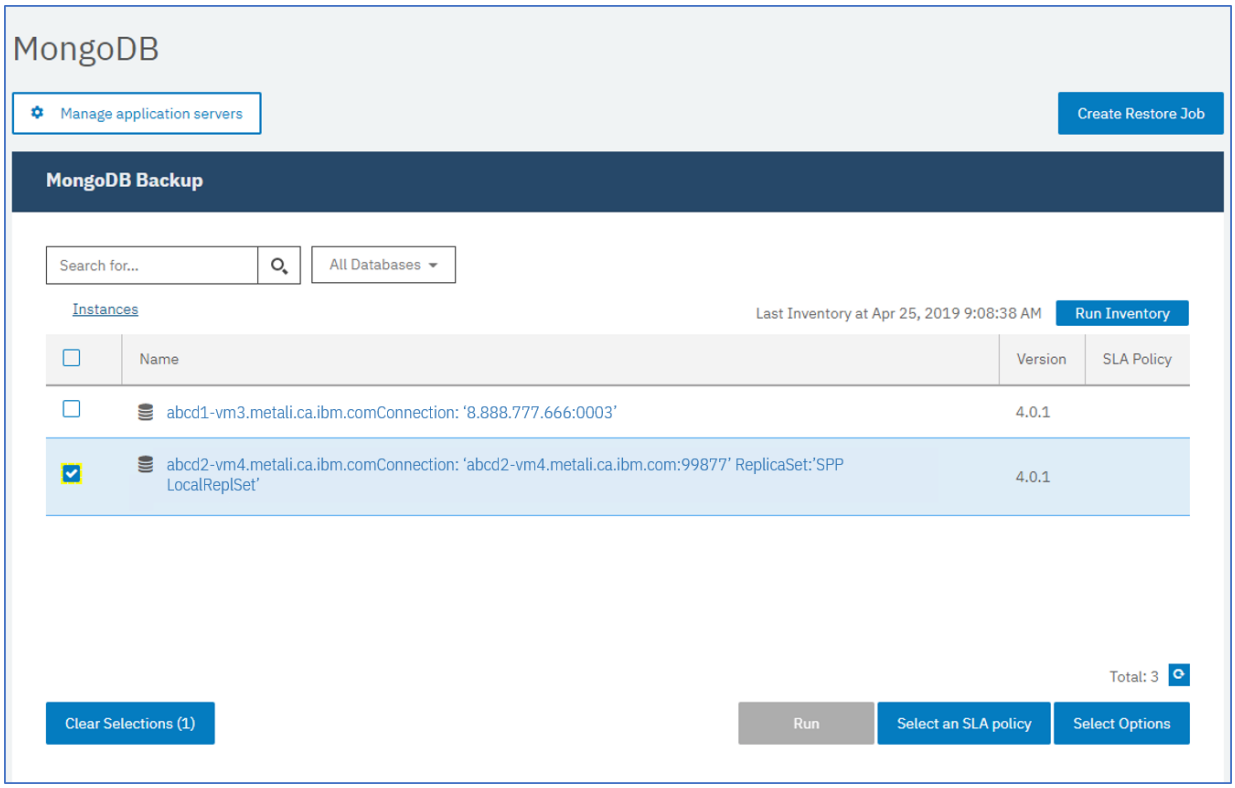


Abbildung 26. Fenster "MongoDB-Sicherung" mit Instanzen

3. Klicken Sie auf **SLA-Richtlinie auswählen** und wählen Sie eine SLA-Richtlinie aus. Speichern Sie Ihre Auswahl.

   Die vordefinierten Auswahlmöglichkeiten sind "Gold", "Silber" und "Bronze". Sie verfügen über verschiedene Häufigkeiten und Aufbewahrungsraten. Sie können auch eine angepasste SLA-Richtlinie erstellen, indem Sie zu **Richtlinienübersicht** > **SLA-Richtlinie hinzufügen** navigieren.

4. Optional: Sollen mehrere Sicherungsdatenströme aktiviert werden, um den Zeitaufwand für das Sichern großer Datenbanken zu reduzieren, klicken Sie auf **Optionen auswählen** und geben Sie die Anzahl paralleler Datenströme ein. Speichern Sie Ihre Änderungen.

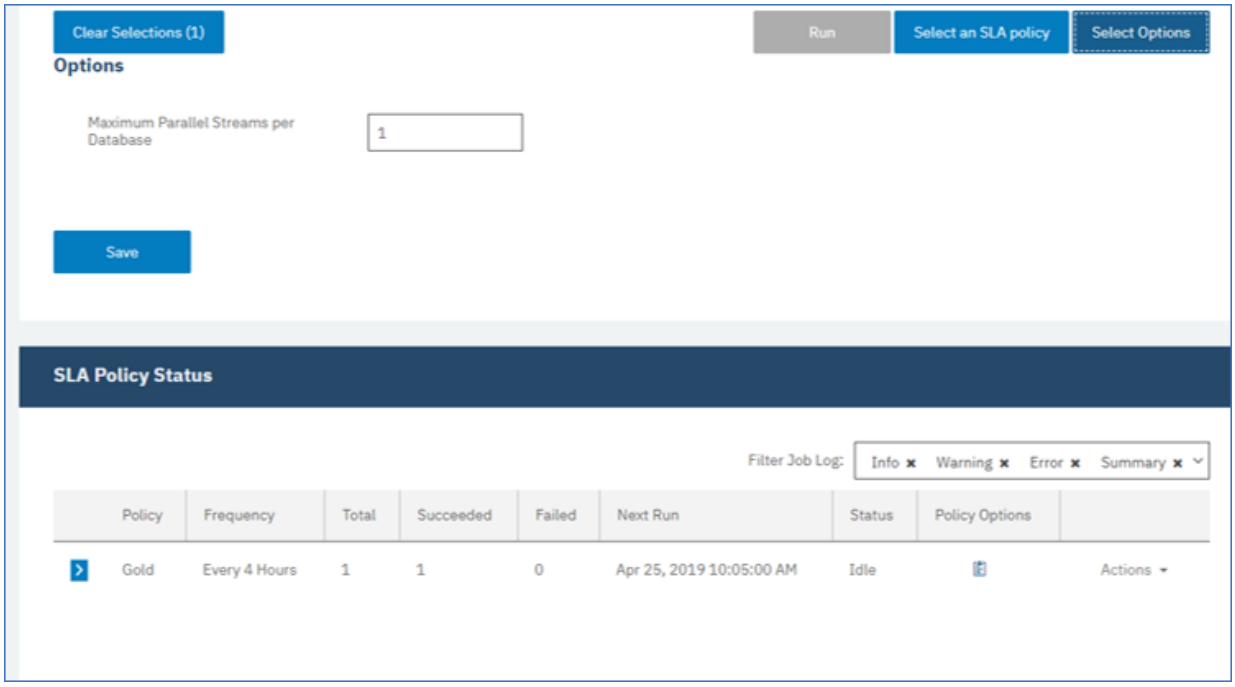


Abbildung 27. Sicherungsoptionen und SLA-Richtlinienstatus

5. Konfigurieren Sie die SLA-Richtlinie, indem Sie auf das Symbol in der Spalte **Richtlinienoptionen** der Tabelle **SLA-Richtlinienstatus** klicken.

   Weitere Informationen zu SLA-Konfigurationsoptionen finden Sie in „SLA-Konfigurationsoptionen für Ihre Sicherung definieren" auf Seite 216.

6. Soll die Richtlinie außerhalb des geplanten Jobs ausgeführt werden, wählen Sie die Instanz aus. Klicken Sie auf die Schaltfläche **Aktionen** und wählen Sie **Starten** aus. Der Status für die ausgewählte SLA-Richtlinie wird in **Aktiv** geändert, und Sie können den Fortschritt des Jobs im angezeigten Protokoll verfolgen.

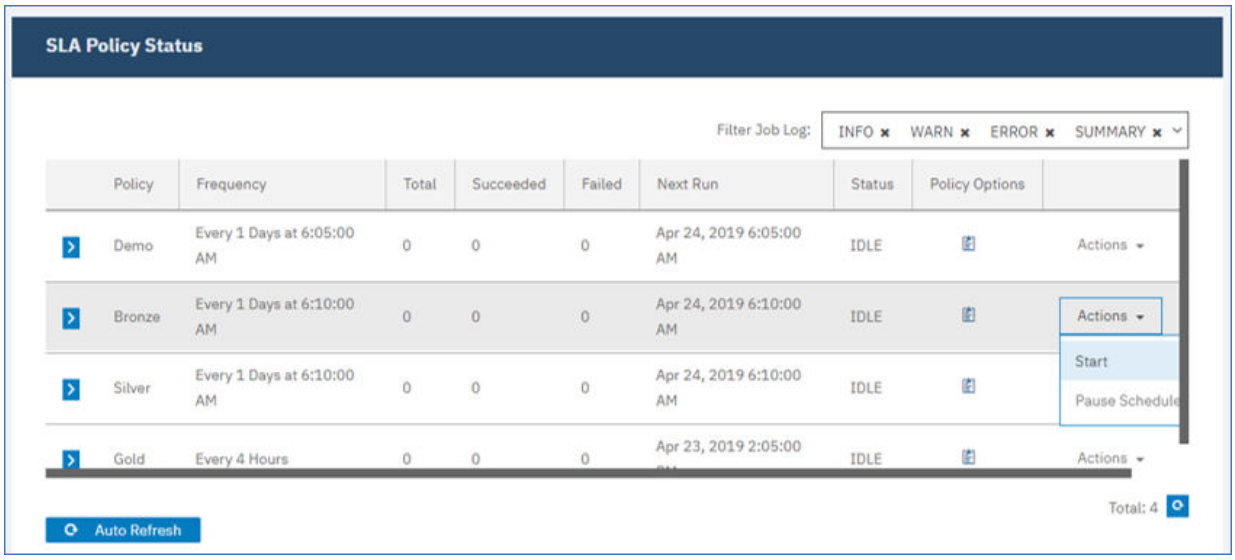


Abbildung 28. SLA-Richtlinien

Nächste Schritte

Nachdem die SLA-Richtlinie gespeichert wurde, können Sie die Richtlinie zu jeder Zeit ausführen, indem Sie auf **Aktionen** neben dem Richtliniennamen klicken und **Starten** auswählen. Der Status im Protokoll ändert sich, um anzuzeigen, dass sich der Sicherungsjob im Status `Aktiv` befindet.

Um einen aktiven Job abzubrechen, klicken Sie auf **Aktionen** neben dem Richtliniennamen und wählen Sie **Abbrechen** aus. In einer Nachricht wird gefragt, ob die Daten aufbewahrt werden sollen, die bereits gesichert wurden. Wählen Sie **Ja** aus, um die gesicherten Daten aufzubewahren, oder wählen Sie **Nein** aus, um die Sicherung zu löschen.

SLA-Konfigurationsoptionen für Ihre Sicherung definieren

Nachdem Sie eine SLA-Richtlinie (SLA = Service-Level-Agreement) für Ihren Sicherungsjob definiert haben, können Sie Zusatzoptionen für diesen Job konfigurieren. Zu den zusätzlichen SLA-Optionen gehören die Ausführung von Scripts und das Erzwingen einer vollständigen Basissicherung.

Vorgehensweise

1. Klicken Sie in der Spalte **Richtlinienoptionen** der Tabelle **SLA-Richtlinienstatus** für den Job, den Sie konfigurieren, auf das Zwischenablagesymbol , um zusätzliche Konfigurationsoptionen anzugeben. Ist der Job bereits konfiguriert, klicken Sie auf das Symbol, um die Konfiguration zu editieren.

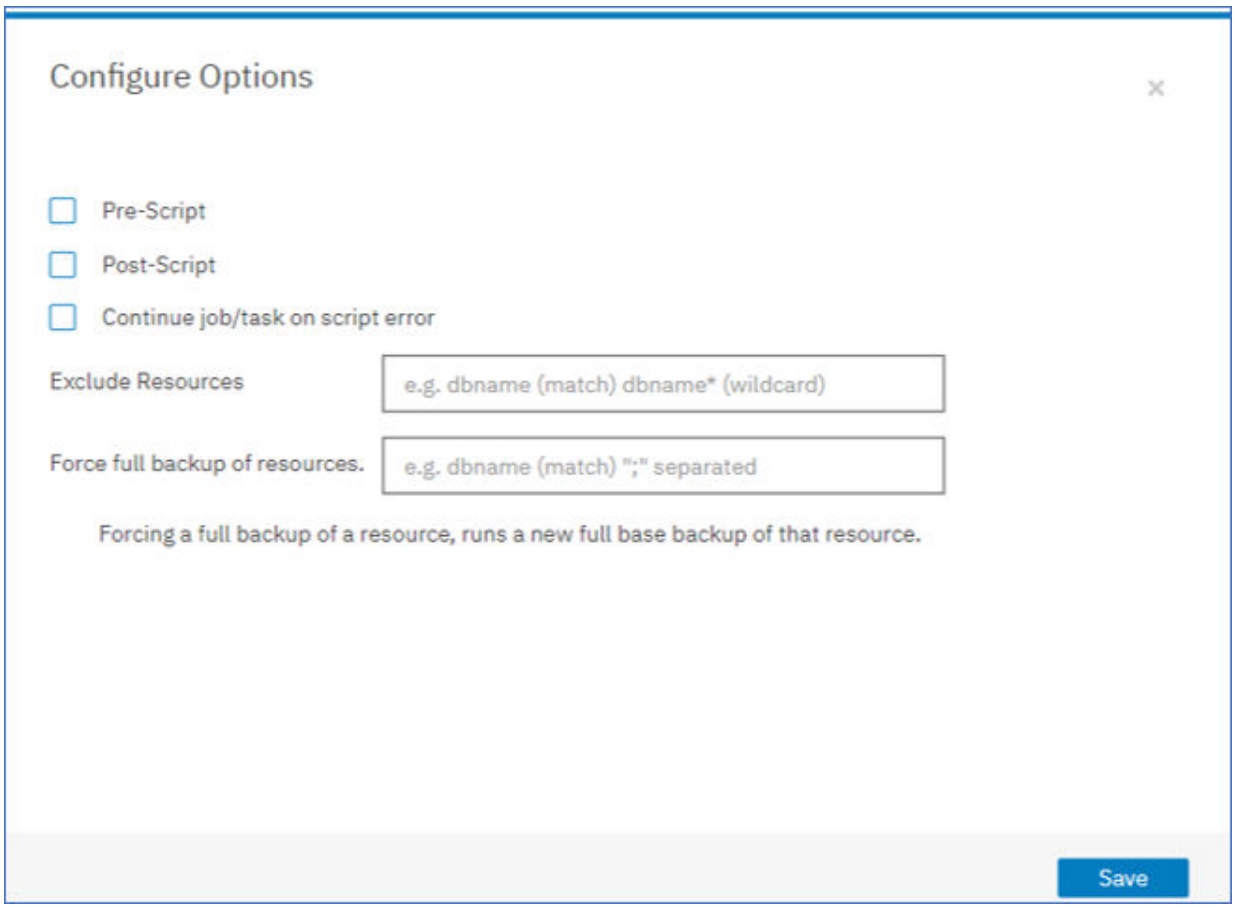


Abbildung 29. Zusätzliche SLA-Konfigurationsoptionen angeben

2. Klicken Sie auf **Vorscript** und definieren Sie die Vorscriptkonfiguration, indem Sie eine der folgenden Optionen auswählen:
   - Klicken Sie auf **Scriptserver verwenden** und wählen Sie ein hochgeladenes Script aus dem Menü aus.

- Klicken Sie nicht auf **Scriptserver verwenden**. Wählen Sie einen Anwendungsserver aus der Liste aus, um das Script an dieser Position auszuführen.

3. Klicken Sie auf **Nachscript** und definieren Sie die Nachscriptkonfiguration, indem Sie eine der folgenden Optionen auswählen:
   - Klicken Sie auf **Scriptserver verwenden** und wählen Sie ein hochgeladenes Script aus dem Menü aus.
   - Klicken Sie nicht auf **Scriptserver verwenden**. Wählen Sie einen Anwendungsserver aus der Liste aus, um das Script an dieser Position auszuführen.

   Scripts und Scriptserver werden auf der Seite **Systemkonfiguration** > **Script** konfiguriert. Weitere Informationen zum Arbeiten mit Scripts finden Sie in **Scripts konfigurieren**.
4. Um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt, wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus.

   Wenn diese Option ausgewählt wird und das Script die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird nach einem anfänglichen Fehlschlagen erneut versucht, die Sicherungs- oder Zurückschreibungsoperation auszuführen, und der Taskstatus des Scripts wird als ABGESCHLOSSEN zurückgemeldet. Wenn diese Option nicht ausgewählt wird, wird nicht erneut versucht, die Sicherung oder Zurückschreibung auszuführen, und der Taskstatus des Scripts wird als FEHLGESCHLAGEN zurückgemeldet.
5. Überspringen Sie **Ressourcen ausschließen** in den MongoDB-SLA-Optionen, da keine auszuschließenden Ressourcen angegeben werden können. Instanzen werden anstelle einzelner Datenbanken gesichert.
6. Um eine neue Gesamtsicherung einer MongoDB-Instanz zu erstellen, wählen Sie **Gesamtsicherung der Ressourcen erzwingen** aus.

   Eine neue Gesamtsicherung dieser Ressource wird erstellt, die einmalig die vorhandene Sicherung dieser Ressource ersetzt. Danach wird die Ressource wie zuvor mit Teilsicherungen gesichert.

MongoDB-Daten zurückschreiben

Um Daten zurückzuschreiben, definieren Sie einen Job, mit dem Daten aus der neuesten Sicherung zurückgeschrieben werden, oder wählen Sie eine frühere Sicherungskopie aus. Wählen Sie aus, ob Daten in die ursprüngliche Instanz oder in eine alternative Instanz auf einer anderen Maschine zurückgeschrieben werden sollen, wobei eine geklonte Kopie erstellt wird. Definieren und speichern Sie den Zurückschreibungsjob, der als Ad-hoc-Operation oder regelmäßig als geplanter Job ausgeführt werden soll.

Vorbereitende Schritte

Bevor Sie einen Zurückschreibungsjob für MongoDB erstellen, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Mindestens ein MongoDB-Sicherungsjob ist definiert und wird erfolgreich ausgeführt. Anweisungen zum Definieren eines Sicherungsjobs finden Sie in „MongoDB-Daten sichern” auf Seite 213.
- IBM Spectrum Protect Plus-Rollen und -Ressourcengruppen sind dem Benutzer zugeordnet, der den Zurückschreibungsjob definiert. Anweisungen zum Zuordnen von Rollen finden Sie in Kapitel 13, „Benutzerzugriff verwalten”, auf Seite 311 und „Rollen für MongoDB” auf Seite 206.
- Auf dem Zielserver ist genügend Plattenspeicher für die Zurückschreibungsoperation zugeordnet.
- Dedizierte Datenträger sind für Dateikopieroperationen zugeordnet.
- Die Ziel- und Quellenserver verfügen über dieselbe Verzeichnisstruktur und dasselbe Layout.
- Bei einer Zurückschreibung aus einem IBM Spectrum Protect-Archiv werden Dateien vom Band in einen Staging-Pool migriert, bevor der Job gestartet wird. Abhängig von der Größe der Zurückschreibung kann dieser Prozess mehrere Stunden dauern.

Für Zurückschreibungsoperationen in alternative Instanzen muss MongoDB auf der Ziel- und Hostmaschine denselben Versionsstand haben.

Weitere Informationen zu den Speichervoraussetzungen finden Sie in Speichervoraussetzungen für MongoDB-Schutz. Weitere Informationen zu den Voraussetzungen und zur Konfiguration finden Sie in Voraussetzungen für MongoDB.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen MongoDB-Zurückschreibungsjob zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **MongoDB** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch starten, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **MongoDB** klicken.
   - Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Symbol .
   - Wenn die optionalen Seiten im Assistenten übergangen werden sollen, wählen Sie **Optionale Schritte überspringen** aus.
2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Schritte aus:
   a) Klicken Sie in der Liste auf eine Quelle, um die Datenbanken anzuzeigen, die für Zurückschreibungsoperationen verfügbar sind. Sie können auch die Suchfunktion verwenden, um nach verfügbaren Instanzen zu suchen, und mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen wechseln.

   b) Klicken Sie auf das Symbol neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll. Sie können mehrere Datenbanken aus der Liste auswählen.

   Die ausgewählten Quellen werden der Zurückschreibungsliste neben der Datenbankliste hinzugefügt. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Symbol neben dem Eintrag.

   c) Klicken Sie auf **Weiter**, um fortzufahren.
3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der Datenbank an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren.

Option	Bezeichnung
Typ der Zurückschreibung	Wählen Sie den Typ des auszuführenden Zurückschreibungsjobs aus. **Bedarfsgesteuert: Momentaufnahme** Führt eine einmalige Zurückschreibungsoperation aus einer Momentaufnahmesicherung aus. **Bedarfsgesteuert: Zeitpunkt** Führt eine einmalige Zurückschreibungsoperation aus einer bestimmten Sicherung nach Zeitpunkt aus. **Wiederholt auftretend** Führt geplante Zurückschreibungsoperationen für Daten von den neuesten Zurückschreibungspunkten aus.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position für die Zurückschreibung aus: **Site** Schreibt Daten von einer Site zurück, die dem Sicherungsspeicherserver zugeordnet ist. **Cloudauslagerung** Schreibt Daten zurück, die im Cloudspeicher gespeichert sind.

Option	Bezeichnung
	Repository-Auslagerung Schreibt Daten zurück, die im Repository-Server gespeichert sind. **Cloudarchivierung** Schreibt Daten zurück, die im Cloudspeicher archiviert sind. **Repository-Archivierung** Schreibt Daten zurück, die im Repository-Server archiviert sind.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus: **Demo** Schreibt Daten von dem vSnap-Demonstrationsserver zurück, der für Testzwecke konfiguriert ist. **Primär** Schreibt Daten von dem vSnap-Server zurück, der das primäre Sicherungsziel ist. **Sekundär** Schreibt Daten von dem vSnap-Server zurück, der das sekundäre Sicherungsziel ist. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, müssen Sie keine Auswahl vornehmen, da die Position bereits ausgewählt ist.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Zurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Zurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datumsbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben, wenn Sie einen bestimmten Zurückschreibungspunkt aus einer Cloudressource oder von einem Repository-Server zurückschreiben, und wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway für die Zurückschreibungsoperation auswählen.

4. Wählen Sie auf der Seite **Ziel definieren In ursprüngliche Instanz zurückschreiben** aus, um Daten auf den ursprünglichen Server zurückzuschreiben, oder wählen Sie **In alternative Instanz zurückschreiben** aus, um Daten an eine andere Position zurückzuschreiben, die Sie aus den aufgelisteten Positionen auswählen können.

   Weitere Informationen zum Zurückschreiben von Daten in die ursprüngliche Instanz finden Sie in In ursprüngliche Instanz zurückschreiben. Weitere Informationen zum Zurückschreiben von Daten in eine alternative Instanz finden Sie in In alternative Instanz zurückschreiben.

5. Wählen Sie auf der Seite **Zurückschreibungsmethode** den Typ der Zurückschreibungsoperation aus und klicken Sie auf **Weiter**, um fortzufahren.

   - **Test**: In diesem Modus erstellt der Agent eine Datenbank, indem er die Datendateien direkt aus dem vSnap-Repository verwendet. Diese Option ist nur verfügbar, wenn Daten in eine alternative Instanz zurückgeschrieben werden. Mitglieder von Replikatgruppen werden nicht rekonfiguriert,

nachdem der MongoDB-Server gestartet wurde. Der Server wird als Einzelknotenreplikatgruppe gestartet.

- **Produktion**: In diesem Modus kopiert der MongoDB-Anwendungsserver zunächst die Dateien aus dem vSnap-Repository auf den Zielhost. Die kopierten Daten werden dann verwendet, um die Datenbank zu starten. MongoDB-Instanzen, die Mitglieder einer Replikatgruppe sind, werden während einer Produktionszurückschreibungsoperation nicht gestartet. Diese Aktion verhindert, dass Daten überschrieben werden, wenn die Verbindung zur Replikatgruppe hergestellt wird.
- **Instant Access**: In diesem Modus wird keine weitere Aktion ausgeführt, nachdem IBM Spectrum Protect Plus die Freigabe bereitgestellt hat. Verwenden Sie die Daten für die angepasste Wiederherstellung aus den Dateien in dem vSnap-Repository.

Für den Testmodus oder Produktionsmodus können Sie wahlweise einen neuen Namen für die zurückgeschriebene Datenbank eingeben.

Für den Produktionsmodus können Sie außerdem einen neuen Ordner für die zurückgeschriebene Datenbank angeben, indem Sie die Datenbank erweitern und einen neuen Ordnernamen eingeben.

6. Optional: Konfigurieren Sie auf der Seite **Joboptionen** weitere Optionen für den Zurückschreibungsjob und klicken Sie auf **Weiter**, um fortzufahren.

   Im Abschnitt **Wiederherstellungsoptionen** ist standardmäßig **Bis zum Ende der Sicherung wiederherstellen** für MongoDB ausgewählt. Mit dieser Option werden die ausgewählten Daten mit dem Status zum Zeitpunkt der Erstellung der Sicherung wiederhergestellt. Die Wiederherstellungsoperation verwendet die Protokolldateien, die in die MongoDB-Sicherung eingeschlossen sind.

   Anwendungsoptionen

   Definieren Sie die Anwendungsoptionen:

   Vorhandene Datenbanken überschreiben

   Aktivieren Sie diese Option, um dem Zurückschreibungsjob das Überschreiben der ausgewählten Datenbank zu ermöglichen. Wird diese Option nicht ausgewählt, schlägt der Zurückschreibungsjob fehl, wenn Daten mit demselben Namen während des Zurückschreibungsprozesses gefunden werden.

   Achtung: Stellen Sie sicher, dass keine anderen Daten dasselbe lokale Datenbankverzeichnis wie die ursprünglichen Daten gemeinsam nutzen, da die Daten überschrieben werden.

   Maximale Anzahl paralleler Datenströme pro Datenbank

   Definieren Sie die maximale Anzahl Datenströme pro Datenbank aus dem Sicherungsspeicher. Diese Einstellung gilt für jede Datenbank in der Jobdefinition. Mehrere Datenbanken können auch dann parallel zurückgeschrieben werden, wenn der Wert der Option auf 1 gesetzt wird. Mehrere parallele Datenströme können Zurückschreibungsoperationen beschleunigen, die Nutzung hoher Bandbreite kann sich jedoch auf die Systemgesamtleistung auswirken.

   Diese Option ist nur gültig, wenn Sie eine MongoDB-Datenbank mit ihrem ursprünglichen Datenbanknamen an die ursprüngliche Position zurückschreiben.

   Erweiterte Optionen

   Definieren Sie die erweiterten Jobdefinitionsoptionen:

   Bereinigung direkt beim Fehlschlagen des Jobs ausführen

   Diese Option wird standardmäßig ausgewählt, um zugeordnete Ressourcen automatisch im Rahmen einer Zurückschreibungsoperation zu bereinigen, wenn die Wiederherstellung fehlschlägt.

   Sitzungsüberschreibung zulassen

   Wählen Sie diese Option aus, um vorhandene Datenbanken mit demselben Namen während einer Zurückschreibungsoperation zu ersetzen. Während einer Instant Disk Restore-Operation wird die vorhandene Datenbank heruntergefahren und überschrieben; anschließend wird die wiederhergestellte Datenbank erneut gestartet. Wenn diese Option nicht ausgewählt wird und eine Datenbank mit demselben Namen gefunden wird, schlägt die Zurückschreibungsoperation mit einem Fehler fehl.

Mit Zurückschreibungen der anderen ausgewählten Datenbanken fortfahren, auch wenn eine Zurückschreibung fehlschlägt
Wenn eine Datenbank in der Instanz nicht erfolgreich zurückgeschrieben wird, wird die Zurückschreibungsoperation für alle anderen Daten, die zurückgeschrieben werden, fortgesetzt. Wird diese Option nicht ausgewählt, wird der Zurückschreibungsjob gestoppt, wenn die Wiederherstellung einer Ressource fehlschlägt.

Mountpunktpräfix
Geben Sie für **Instant Access**-Zurückschreibungsoperationen ein Mountpunktpräfix für den Pfad an, für den der Mountpunkt bereitgestellt werden soll.

7. Optional: Geben Sie auf der Seite **Scripts anwenden** Scripts an, die vor oder nach der Ausführung eines Jobs ausgeführt werden können. Batch- und PowerShell-Scripts werden unter Windows-Betriebssystemen unterstützt, während Shell-Scripts unter Linux-Betriebssystemen unterstützt werden.

   Vorscript
   Wählen Sie dieses Kontrollkästchen aus, um ein hochgeladenes Script und einen Anwendungs- oder Scriptserver auszuwählen, auf dem das Vorscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Um Scripts und Scriptserver zu konfigurieren, klicken Sie auf **Systemkonfiguration** > **Script**.

   Nachscript
   Wählen Sie diese Option aus, um ein hochgeladenes Script und einen Anwendungs- oder Scriptserver auszuwählen, auf dem das Nachscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Um Scripts und Scriptserver zu konfigurieren, klicken Sie auf die Seite **Systemkonfiguration** > **Script**.

   Job/Task bei Scriptfehler fortsetzen
   Wählen Sie diese Option aus, um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt. Wenn diese Option aktiviert wird, wird für den Fall, dass die Verarbeitung eines Scripts mit einem Rückkehrcode ungleich null beendet wird, die Ausführung des Sicherungs- oder Zurückschreibungsjobs fortgesetzt und der Taskstatus für das Vorscript als ABGESCHLOSSEN zurückgemeldet. Wenn ein Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird der Taskstatus für das Nachscript als ABGESCHLOSSEN zurückgemeldet. Wenn diese Option nicht ausgewählt wird, wird der Sicherungs- oder Zurückschreibungsjob nicht ausgeführt und für die Vorscript- oder Nachscript-Task wird FEHLGESCHLAGEN zurückgemeldet.

   Klicken Sie auf **Weiter**, um fortzufahren.
8. Klicken Sie auf der Seite **Zeitplan** auf **Weiter**, um bedarfsgesteuerte Jobs nach Beendigung des Assistenen "Momentaufnahmezurückschreibung" zu starten. Geben Sie für sich wiederholende Jobs einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an.
9. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs.

   Achtung: Überprüfen Sie die ausgewählten Optionen, bevor Sie mit **Übergeben** fortfahren, da Daten überschrieben werden, wenn die Anwendungsoption **Vorhandene Daten überschreiben** ausgewählt ist. Sie können einen Zurückschreibungsjob abbrechen, wenn er in Bearbeitung ist. Wenn die Option **Vorhandene Daten überschreiben** ausgewählt ist, werden Daten jedoch auch dann überschrieben, wenn Sie den Job abbrechen.

10. Um den Job fortzusetzen, klicken Sie auf **Übergeben**. Um den Job abzubrechen, navigieren Sie zu **Jobs und Operationen** und klicken Sie auf die Registerkarte **Zeitplan**. Suchen Sie nach dem Zurückschreibungsjob, der abgebrochen werden soll. Klicken Sie auf **Aktionen** und wählen Sie **Abbrechen** aus.

Ergebnisse

Wenige Augenblicke nach der Auswahl von **Zurückschreiben** wird der Job des Typs **Bedarfsgesteuerte Zurückschreibung** dem Fenster **Jobs und Operationen** > **Aktive Jobs** hinzugefügt. Klicken Sie auf den Satz, um die Details zu den Operationsschritten anzuzeigen. Sie können auch die komprimierte Protokolldatei herunterladen, indem Sie auf **ZIP-Datei herunterladen** klicken. Klicken Sie für alle anderen Jobs

auf die Registerkarte **Aktive Jobs** oder **Jobprotokoll**; klicken Sie dann auf den Job, um die zugehörigen Details anzuzeigen.

Die IP-Adresse und der Port für den zurückgeschriebenen Server sind in der Protokolldatei für die Zurückschreibungsoperation enthalten. Navigieren Sie zu **Jobs und Operationen** > **Aktive Jobs**, um nach den Protokollen für die Zurückschreibungsoperation zu suchen.

Informationen zum Zurückschreiben von Daten in die ursprüngliche Instanz finden Sie in In ursprüngliche Instanz zurückschreiben. Informationen zum Zurückschreiben von Daten in eine alternative Instanz finden Sie in In alternative Instanz zurückschreiben.

MongoDB-Daten in die ursprüngliche Instanz zurückschreiben
Sie können eine MongoDB-Instanz auf den ursprünglichen Host zurückschreiben und zwischen einer Zurückschreibung der neuesten Sicherung oder einer früheren Version einer MongoDB-Datenbanksicherung wählen. Wenn Sie Daten in ihre ursprüngliche Instanz zurückschreiben, können Sie sie nicht umbenennen. Mit dieser Zurückschreibungsoption wird eine vollständige Produktionsdatenzurückschreibung ausgeführt, und die vorhandenen Daten werden an der Zielsite überschrieben, wenn die Anwendungsoption **Vorhandene Datenbanken überschreiben** ausgewählt wird.

Vorbereitende Schritte

Bevor Sie einen Zurückschreibungsjob für MongoDB erstellen, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Mindestens ein MongoDB-Sicherungsjob ist definiert und wird erfolgreich ausgeführt. Anweisungen zum Definieren eines Sicherungsjobs finden Sie in „MongoDB-Daten sichern” auf Seite 213.
- IBM Spectrum Protect Plus-Rollen und -Ressourcengruppen sind dem Benutzer zugeordnet, der den Zurückschreibungsjob definiert. Anweisungen zum Zuordnen von Rollen finden Sie in Kapitel 13, „Benutzerzugriff verwalten”, auf Seite 311 und „Rollen für MongoDB” auf Seite 206.
- Auf dem Zielserver ist genügend Plattenspeicher für die Zurückschreibungsoperation zugeordnet.
- Dedizierte Datenträger sind für Dateikopieroperationen zugeordnet.
- Die Ziel- und Quellenserver verfügen über dieselbe Verzeichnisstruktur und dasselbe Layout.
- Bei einer Zurückschreibung aus einem IBM Spectrum Protect-Archiv werden Dateien vom Band in einen Staging-Pool migriert, bevor der Job gestartet wird. Abhängig von der Größe der Zurückschreibung kann dieser Prozess mehrere Stunden dauern.

Weitere Informationen zu den Speichervoraussetzungen finden Sie in Speichervoraussetzungen für MongoDB-Schutz. Weitere Informationen zu den Voraussetzungen und zur Konfiguration finden Sie in Voraussetzungen für MongoDB.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **MongoDB** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch starten, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **MongoDB** klicken.
   - Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Symbol  .
   - Wenn die optionalen Seiten im Assistenten übergangen werden sollen, wählen Sie **Optionale Schritte überspringen** aus.
2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Schritte aus:
   a) Klicken Sie in der Liste auf eine Quelle, um die Datenbanken anzuzeigen, die für Zurückschreibungsoperationen verfügbar sind. Sie können auch die Suchfunktion verwenden, um nach verfügbaren Instanzen zu suchen, und mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen wechseln.

b) Klicken Sie auf das Symbol  neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll. Sie können mehrere Datenbanken aus der Liste auswählen.

   Die ausgewählten Quellen werden der Zurückschreibungsliste neben der Datenbankliste hinzugefügt. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Symbol  neben dem Eintrag.

c) Klicken Sie auf **Weiter**, um fortzufahren.

3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der Datenbank an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren.

Option	Bezeichnung
Typ der Zurückschreibung	Wählen Sie den Typ des auszuführenden Zurückschreibungsjobs aus. **Bedarfsgesteuert: Momentaufnahme** Führt eine einmalige Zurückschreibungsoperation aus einer Momentaufnahmesicherung aus. **Bedarfsgesteuert: Zeitpunkt** Führt eine einmalige Zurückschreibungsoperation aus einer bestimmten Sicherung nach Zeitpunkt aus. **Wiederholt auftretend** Führt geplante Zurückschreibungsoperationen für Daten von den neuesten Zurückschreibungspunkten aus.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position für die Zurückschreibung aus: **Site** Schreibt Daten von einer Site zurück, die dem Sicherungsspeicherserver zugeordnet ist. **Cloudauslagerung** Schreibt Daten zurück, die im Cloudspeicher gespeichert sind. **Repository-Auslagerung** Schreibt Daten zurück, die im Repository-Server gespeichert sind. **Cloudarchivierung** Schreibt Daten zurück, die im Cloudspeicher archiviert sind. **Repository-Archivierung** Schreibt Daten zurück, die im Repository-Server archiviert sind.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus: **Demo** Schreibt Daten von dem vSnap-Demonstrationsserver zurück, der für Testzwecke konfiguriert ist. **Primär** Schreibt Daten von dem vSnap-Server zurück, der das primäre Sicherungsziel ist. **Sekundär** Schreibt Daten von dem vSnap-Server zurück, der das sekundäre Sicherungsziel ist. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, müssen Sie keine Auswahl vornehmen, da die Position bereits ausgewählt ist.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Zurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.

Option	Bezeichnung
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Zurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datumsbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben, wenn Sie einen bestimmten Zurückschreibungspunkt aus einer Cloudressource oder von einem Repository-Server zurückschreiben, und wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway für die Zurückschreibungsoperation auswählen.

4. Wählen Sie auf der Seite "Ziel definieren" **In ursprüngliche Instanz zurückschreiben** aus und klicken Sie auf **Weiter**.
5. Wählen Sie auf der Seite **Zurückschreibungsmethode** den Typ der Zurückschreibungsoperation aus und klicken Sie auf **Weiter**, um fortzufahren.
   - **Produktion**

     Um eine vollständige Instanz in die ursprüngliche Instanz wiederherzustellen, ist die bevorzugte Methode die Auswahl dieser Option zusammen mit der Anwendungsoption zum Überschreiben. MongoDB-Instanzen, die Mitglieder einer Replikatgruppe sind, werden während einer Produktionszurückschreibungsoperation nicht gestartet. Diese Aktion verhindert, dass Daten überschrieben werden, wenn die Verbindung zur Replikatgruppe hergestellt wird.
   - **Test**

     Wählen Sie diese Option aus, um Daten auf denselben Server, aber unter Verwendung eines anderen Ports, zurückzuschreiben.
   - **Instant Access**

     Wählen Sie diese Option aus, um die Sicherung für den Anwendungsserver bereitzustellen, ohne dass die Daten zurückgeschrieben oder überschrieben werden.

     Klicken Sie auf **Weiter**, um fortzufahren.

   Für den Testmodus oder Produktionsmodus können Sie wahlweise einen neuen Namen für die zurückgeschriebene Datenbank eingeben.

   Für den Produktionsmodus können Sie außerdem einen neuen Ordner für die zurückgeschriebene Datenbank angeben, indem Sie die Datenbank erweitern und einen neuen Ordnernamen eingeben.
6. Optional: Konfigurieren Sie auf der Seite **Joboptionen** weitere Optionen für den Zurückschreibungsjob und klicken Sie auf **Weiter**, um fortzufahren.

   Im Abschnitt **Wiederherstellungsoptionen** ist standardmäßig **Bis zum Ende der Sicherung wiederherstellen** für MongoDB ausgewählt. Mit dieser Option werden die ausgewählten Daten mit dem Status zum Zeitpunkt der Erstellung der Sicherung wiederhergestellt. Die Wiederherstellungsoperation verwendet die Protokolldateien, die in die MongoDB-Sicherung eingeschlossen sind.

   Anwendungsoptionen
   Definieren Sie die Anwendungsoptionen:

   Vorhandene Datenbanken überschreiben
   Aktivieren Sie diese Option, um dem Zurückschreibungsjob das Überschreiben der ausgewählten Datenbank zu ermöglichen. Wird diese Option nicht ausgewählt, schlägt der Zurück-

schreibungsjob fehl, wenn Daten mit demselben Namen während des Zurückschreibungsprozesses gefunden werden.

Achtung: Stellen Sie sicher, dass keine anderen Daten dasselbe lokale Datenbankverzeichnis wie die ursprünglichen Daten gemeinsam nutzen, da die Daten überschrieben werden.

Maximale Anzahl paralleler Datenströme pro Datenbank
Definieren Sie die maximale Anzahl Datenströme pro Datenbank aus dem Sicherungsspeicher. Diese Einstellung gilt für jede Datenbank in der Jobdefinition. Mehrere Datenbanken können auch dann parallel zurückgeschrieben werden, wenn der Wert der Option auf 1 gesetzt wird. Mehrere parallele Datenströme können Zurückschreibungsoperationen beschleunigen, die Nutzung hoher Bandbreite kann sich jedoch auf die Systemgesamtleistung auswirken.

Diese Option ist nur gültig, wenn Sie eine MongoDB-Datenbank mit ihrem ursprünglichen Datenbanknamen an die ursprüngliche Position zurückschreiben.

Erweiterte Optionen
Definieren Sie die erweiterten Jobdefinitionsoptionen:

Bereinigung direkt beim Fehlschlagen des Jobs ausführen
Diese Option wird standardmäßig ausgewählt, um zugeordnete Ressourcen automatisch im Rahmen einer Zurückschreibungsoperation zu bereinigen, wenn die Wiederherstellung fehlschlägt.

Sitzungsüberschreibung zulassen
Wählen Sie diese Option aus, um vorhandene Datenbanken mit demselben Namen während einer Zurückschreibungsoperation zu ersetzen. Während einer Instant Disk Restore-Operation wird die vorhandene Datenbank heruntergefahren und überschrieben; anschließend wird die wiederhergestellte Datenbank erneut gestartet. Wenn diese Option nicht ausgewählt wird und eine Datenbank mit demselben Namen gefunden wird, schlägt die Zurückschreibungsoperation mit einem Fehler fehl.

Mit Zurückschreibungen der anderen ausgewählten Datenbanken fortfahren, auch wenn eine Zurückschreibung fehlschlägt
Wenn eine Datenbank in der Instanz nicht erfolgreich zurückgeschrieben wird, wird die Zurückschreibungsoperation für alle anderen Daten, die zurückgeschrieben werden, fortgesetzt. Wird diese Option nicht ausgewählt, wird der Zurückschreibungsjob gestoppt, wenn die Wiederherstellung einer Ressource fehlschlägt.

Mountpunktpräfix
Geben Sie für **Instant Access**-Zurückschreibungsoperationen ein Mountpunktpräfix für den Pfad an, für den der Mountpunkt bereitgestellt werden soll.

7. Optional: Geben Sie auf der Seite **Scripts anwenden** Scripts an, die vor oder nach der Ausführung eines Jobs ausgeführt werden können. Batch- und PowerShell-Scripts werden unter Windows-Betriebssystemen unterstützt, während Shell-Scripts unter Linux-Betriebssystemen unterstützt werden.

Vorscript
Wählen Sie dieses Kontrollkästchen aus, um ein hochgeladenes Script und einen Anwendungs- oder Scriptserver auszuwählen, auf dem das Vorscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Um Scripts und Scriptserver zu konfigurieren, klicken Sie auf **Systemkonfiguration** > **Script**.

Nachscript
Wählen Sie diese Option aus, um ein hochgeladenes Script und einen Anwendungs- oder Scriptserver auszuwählen, auf dem das Nachscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Um Scripts und Scriptserver zu konfigurieren, klicken Sie auf die Seite **Systemkonfiguration** > **Script**.

Job/Task bei Scriptfehler fortsetzen
Wählen Sie diese Option aus, um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt. Wenn diese Option aktiviert wird, wird für den Fall, dass die Verarbeitung eines Scripts mit einem Rückkehrcode ungleich null beendet wird, die Ausführung des Sicherungs- oder Zurückschreibungsjobs fortgesetzt und der Taskstatus für das Vorscript als ABGE-

SCHLOSSEN zurückgemeldet. Wenn ein Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird der Taskstatus für das Nachscript als ABGESCHLOSSEN zurückgemeldet. Wenn diese Option nicht ausgewählt wird, wird der Sicherungs- oder Zurückschreibungsjob nicht ausgeführt und für die Vorscript- oder Nachscript-Task wird FEHLGESCHLAGEN zurückgemeldet.

Klicken Sie auf **Weiter**, um fortzufahren.

8. Klicken Sie auf der Seite **Zeitplan** auf **Weiter**, um bedarfsgesteuerte Jobs nach Beendigung des Assistenen "Momentaufnahmezurückschreibung" zu starten. Geben Sie für sich wiederholende Jobs einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an.
9. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs.

   Achtung: Überprüfen Sie die ausgewählten Optionen, bevor Sie mit **Übergeben** fortfahren, da Daten überschrieben werden, wenn die Anwendungsoption **Vorhandene Daten überschreiben** ausgewählt ist. Sie können einen Zurückschreibungsjob abbrechen, wenn er in Bearbeitung ist. Wenn die Option **Vorhandene Daten überschreiben** ausgewählt ist, werden Daten jedoch auch dann überschrieben, wenn Sie den Job abbrechen.

10. Um den Job fortzusetzen, klicken Sie auf **Übergeben**. Um den Job abzubrechen, navigieren Sie zu **Jobs und Operationen** und klicken Sie auf die Registerkarte **Zeitplan**. Suchen Sie nach dem Zurückschreibungsjob, der abgebrochen werden soll. Klicken Sie auf **Aktionen** und wählen Sie **Abbrechen** aus.

MongoDB-Daten in eine alternative Instanz zurückschreiben

Sie können eine MongoDB-Datenbanksicherung auswählen und auf einen alternativen Host zurückschreiben. Sie können eine Datenbank auch in ein anderes vSnap-Repository zurückschreiben oder die Datenbank umbenennen. Bei diesem Prozess wird eine exakte Kopie der Instanz auf einem anderen Host erstellt.

Vorbereitende Schritte

Bevor Sie einen Zurückschreibungsjob für MongoDB erstellen, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Mindestens ein MongoDB-Sicherungsjob ist definiert und wird erfolgreich ausgeführt. Anweisungen zum Definieren eines Sicherungsjobs finden Sie in „MongoDB-Daten sichern” auf Seite 213.
- IBM Spectrum Protect Plus-Rollen und -Ressourcengruppen sind dem Benutzer zugeordnet, der den Zurückschreibungsjob definiert. Anweisungen zum Zuordnen von Rollen finden Sie in Kapitel 13, „Benutzerzugriff verwalten”, auf Seite 311 und „Rollen für MongoDB” auf Seite 206.
- Auf dem Zielserver ist genügend Plattenspeicher für die Zurückschreibungsoperation zugeordnet.
- Dedizierte Datenträger sind für Dateikopieroperationen zugeordnet.
- Die Ziel- und Quellenserver verfügen über dieselbe Verzeichnisstruktur und dasselbe Layout.
- Bei einer Zurückschreibung aus einem IBM Spectrum Protect-Archiv werden Dateien vom Band in einen Staging-Pool migriert, bevor der Job gestartet wird. Abhängig von der Größe der Zurückschreibung kann dieser Prozess mehrere Stunden dauern.

Für Zurückschreibungsoperationen in alternative Instanzen muss MongoDB auf der Ziel- und Hostmaschine denselben Versionsstand haben.

Weitere Informationen zu den Speichervoraussetzungen finden Sie in Speichervoraussetzungen für MongoDB-Schutz. Weitere Informationen zu den Voraussetzungen und zur Konfiguration finden Sie in Voraussetzungen für MongoDB.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **MongoDB** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

- Sie können den Assistenten "Momentaufnahmezurückschreibung" auch starten, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **MongoDB** klicken.
- Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Symbol .
- Wenn die optionalen Seiten im Assistenten übergangen werden sollen, wählen Sie **Optionale Schritte überspringen** aus.

2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Schritte aus:
   a) Klicken Sie in der Liste auf eine Quelle, um die Datenbanken anzuzeigen, die für Zurückschreibungsoperationen verfügbar sind. Sie können auch die Suchfunktion verwenden, um nach verfügbaren Instanzen zu suchen, und mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen wechseln.
   b) Klicken Sie auf das Symbol neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll. Sie können mehrere Datenbanken aus der Liste auswählen.

      Die ausgewählten Quellen werden der Zurückschreibungsliste neben der Datenbankliste hinzugefügt. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Symbol neben dem Eintrag.
   c) Klicken Sie auf **Weiter**, um fortzufahren.
3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der Datenbank an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren.

Option	Bezeichnung
Typ der Zurückschreibung	Wählen Sie den Typ des auszuführenden Zurückschreibungsjobs aus. **Bedarfsgesteuert: Momentaufnahme** Führt eine einmalige Zurückschreibungsoperation aus einer Momentaufnahmesicherung aus. **Bedarfsgesteuert: Zeitpunkt** Führt eine einmalige Zurückschreibungsoperation aus einer bestimmten Sicherung nach Zeitpunkt aus. **Wiederholt auftretend** Führt geplante Zurückschreibungsoperationen für Daten von den neuesten Zurückschreibungspunkten aus.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position für die Zurückschreibung aus: **Site** Schreibt Daten von einer Site zurück, die dem Sicherungsspeicherserver zugeordnet ist. **Cloudauslagerung** Schreibt Daten zurück, die im Cloudspeicher gespeichert sind. **Repository-Auslagerung** Schreibt Daten zurück, die im Repository-Server gespeichert sind. **Cloudarchivierung** Schreibt Daten zurück, die im Cloudspeicher archiviert sind. **Repository-Archivierung** Schreibt Daten zurück, die im Repository-Server archiviert sind.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus:

Option	Bezeichnung
	Demo Schreibt Daten von dem vSnap-Demonstrationsserver zurück, der für Testzwecke konfiguriert ist. **Primär** Schreibt Daten von dem vSnap-Server zurück, der das primäre Sicherungsziel ist. **Sekundär** Schreibt Daten von dem vSnap-Server zurück, der das sekundäre Sicherungsziel ist. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, müssen Sie keine Auswahl vornehmen, da die Position bereits ausgewählt ist.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Zurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Zurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datumsbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben, wenn Sie einen bestimmten Zurückschreibungspunkt aus einer Cloudressource oder von einem Repository-Server zurückschreiben, und wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway für die Zurückschreibungsoperation auswählen.

4. Wählen Sie auf der Seite **Ziel definieren In alternative Instanz zurückschreiben** aus und wählen Sie die Zielinstanz aus, in die die Daten zurückgeschrieben werden sollen.

   Die ursprüngliche Instanz ist nicht auswählbar, da Sie die ursprünglichen Daten nicht überschreiben können, wenn Sie **In alternative Instanz zurückschreiben** auswählen. Es ist ebenfalls nicht möglich, Instanzen mit anderen Versionsständen oder Instanzen, die sich auf demselben Host wie die ursprüngliche Instanz befinden, auszuwählen.

   Klicken Sie auf **Weiter**, um fortzufahren.
5. Wählen Sie auf der Seite **Zurückschreibungsmethode** den Typ der Zurückschreibungsoperation aus und klicken Sie auf **Weiter**, um fortzufahren.

   - **Test**: In diesem Modus erstellt der Agent eine Datenbank, indem er die Datendateien direkt aus dem vSnap-Repository verwendet. Diese Option ist nur verfügbar, wenn Daten in eine alternative Instanz zurückgeschrieben werden. Mitglieder von Replikatgruppen werden nicht rekonfiguriert, nachdem der MongoDB-Server gestartet wurde. Der Server wird als Einzelknotenreplikatgruppe gestartet.
   - **Produktion**: In diesem Modus kopiert der MongoDB-Anwendungsserver zunächst die Dateien aus dem vSnap-Repository auf den Zielhost. Die kopierten Daten werden dann verwendet, um die Datenbank zu starten. MongoDB-Instanzen, die Mitglieder einer Replikatgruppe sind, werden während einer Produktionszurückschreibungsoperation nicht gestartet. Diese Aktion verhindert, dass Daten überschrieben werden, wenn die Verbindung zur Replikatgruppe hergestellt wird.

- **Instant Access**: In diesem Modus wird keine weitere Aktion ausgeführt, nachdem IBM Spectrum Protect Plus die Freigabe bereitgestellt hat. Verwenden Sie die Daten für die angepasste Wiederherstellung aus den Dateien in dem vSnap-Repository.

Für den Testmodus oder Produktionsmodus können Sie wahlweise einen neuen Namen für die zurückgeschriebene Datenbank eingeben.

Für den Produktionsmodus können Sie außerdem einen neuen Ordner für die zurückgeschriebene Datenbank angeben, indem Sie die Datenbank erweitern und einen neuen Ordnernamen eingeben.

6. Optional: Konfigurieren Sie auf der Seite **Joboptionen** weitere Optionen für den Zurückschreibungsjob und klicken Sie auf **Weiter**, um fortzufahren.

   Im Abschnitt **Wiederherstellungsoptionen** ist standardmäßig **Bis zum Ende der Sicherung wiederherstellen** für MongoDB ausgewählt. Mit dieser Option werden die ausgewählten Daten mit dem Status zum Zeitpunkt der Erstellung der Sicherung wiederhergestellt. Die Wiederherstellungsoperation verwendet die Protokolldateien, die in die MongoDB-Sicherung eingeschlossen sind.

   Anwendungsoptionen

   Definieren Sie die Anwendungsoptionen:

   Vorhandene Datenbanken überschreiben

   Aktivieren Sie diese Option, um dem Zurückschreibungsjob das Überschreiben der ausgewählten Datenbank zu ermöglichen. Wird diese Option nicht ausgewählt, schlägt der Zurückschreibungsjob fehl, wenn Daten mit demselben Namen während des Zurückschreibungsprozesses gefunden werden.

   Achtung: Stellen Sie sicher, dass keine anderen Daten dasselbe lokale Datenbankverzeichnis wie die ursprünglichen Daten gemeinsam nutzen, da die Daten überschrieben werden.

   Maximale Anzahl paralleler Datenströme pro Datenbank

   Definieren Sie die maximale Anzahl Datenströme pro Datenbank aus dem Sicherungsspeicher. Diese Einstellung gilt für jede Datenbank in der Jobdefinition. Mehrere Datenbanken können auch dann parallel zurückgeschrieben werden, wenn der Wert der Option auf 1 gesetzt wird. Mehrere parallele Datenströme können Zurückschreibungsoperationen beschleunigen, die Nutzung hoher Bandbreite kann sich jedoch auf die Systemgesamtleistung auswirken.

   Diese Option ist nur gültig, wenn Sie eine MongoDB-Datenbank mit ihrem ursprünglichen Datenbanknamen an die ursprüngliche Position zurückschreiben.

   Erweiterte Optionen

   Definieren Sie die erweiterten Jobdefinitionsoptionen:

   Bereinigung direkt beim Fehlschlagen des Jobs ausführen

   Diese Option wird standardmäßig ausgewählt, um zugeordnete Ressourcen automatisch im Rahmen einer Zurückschreibungsoperation zu bereinigen, wenn die Wiederherstellung fehlschlägt.

   Sitzungsüberschreibung zulassen

   Wählen Sie diese Option aus, um vorhandene Datenbanken mit demselben Namen während einer Zurückschreibungsoperation zu ersetzen. Während einer Instant Disk Restore-Operation wird die vorhandene Datenbank heruntergefahren und überschrieben; anschließend wird die wiederhergestellte Datenbank erneut gestartet. Wenn diese Option nicht ausgewählt wird und eine Datenbank mit demselben Namen gefunden wird, schlägt die Zurückschreibungsoperation mit einem Fehler fehl.

   Mit Zurückschreibungen der anderen ausgewählten Datenbanken fortfahren, auch wenn eine Zurückschreibung fehlschlägt

   Wenn eine Datenbank in der Instanz nicht erfolgreich zurückgeschrieben wird, wird die Zurückschreibungsoperation für alle anderen Daten, die zurückgeschrieben werden, fortgesetzt. Wird diese Option nicht ausgewählt, wird der Zurückschreibungsjob gestoppt, wenn die Wiederherstellung einer Ressource fehlschlägt.

Mountpunktpräfix
Geben Sie für **Instant Access**-Zurückschreibungsoperationen ein Mountpunktpräfix für den Pfad an, für den der Mountpunkt bereitgestellt werden soll.

7. Optional: Geben Sie auf der Seite **Scripts anwenden** Scripts an, die vor oder nach der Ausführung eines Jobs ausgeführt werden können. Batch- und PowerShell-Scripts werden unter Windows-Betriebssystemen unterstützt, während Shell-Scripts unter Linux-Betriebssystemen unterstützt werden.

   Vorscript
   Wählen Sie dieses Kontrollkästchen aus, um ein hochgeladenes Script und einen Anwendungs- oder Scriptserver auszuwählen, auf dem das Vorscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Um Scripts und Scriptserver zu konfigurieren, klicken Sie auf **Systemkonfiguration** > **Script**.

   Nachscript
   Wählen Sie diese Option aus, um ein hochgeladenes Script und einen Anwendungs- oder Scriptserver auszuwählen, auf dem das Nachscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Um Scripts und Scriptserver zu konfigurieren, klicken Sie auf die Seite **Systemkonfiguration** > **Script**.

   Job/Task bei Scriptfehler fortsetzen
   Wählen Sie diese Option aus, um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt. Wenn diese Option aktiviert wird, wird für den Fall, dass die Verarbeitung eines Scripts mit einem Rückkehrcode ungleich null beendet wird, die Ausführung des Sicherungs- oder Zurückschreibungsjobs fortgesetzt und der Taskstatus für das Vorscript als ABGESCHLOSSEN zurückgemeldet. Wenn ein Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird der Taskstatus für das Nachscript als ABGESCHLOSSEN zurückgemeldet. Wenn diese Option nicht ausgewählt wird, wird der Sicherungs- oder Zurückschreibungsjob nicht ausgeführt und für die Vorscript- oder Nachscript-Task wird FEHLGESCHLAGEN zurückgemeldet.

   Klicken Sie auf **Weiter**, um fortzufahren.

8. Klicken Sie auf der Seite **Zeitplan** auf **Weiter**, um bedarfsgesteuerte Jobs nach Beendigung des Assistenen "Momentaufnahmezurückschreibung" zu starten. Geben Sie für sich wiederholende Jobs einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an.
9. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs.

   Achtung: Überprüfen Sie die ausgewählten Optionen, bevor Sie mit **Übergeben** fortfahren, da Daten überschrieben werden, wenn die Anwendungsoption **Vorhandene Daten überschreiben** ausgewählt ist. Sie können einen Zurückschreibungsjob abbrechen, wenn er in Bearbeitung ist. Wenn die Option **Vorhandene Daten überschreiben** ausgewählt ist, werden Daten jedoch auch dann überschrieben, wenn Sie den Job abbrechen.

10. Um den Job fortzusetzen, klicken Sie auf **Übergeben**. Um den Job abzubrechen, navigieren Sie zu **Jobs und Operationen** und klicken Sie auf die Registerkarte **Zeitplan**. Suchen Sie nach dem Zurückschreibungsjob, der abgebrochen werden soll. Klicken Sie auf **Aktionen** und wählen Sie **Abbrechen** aus.

Operation für differenzierte Zurückschreibung für MongoDB verwenden
Sie können bestimmte MongoDB-Datenbanken oder -Sammlungen mithilfe einer Operation für differenzierte Zurückschreibung zurückschreiben. Bei einer Operation für differenzierte Zurückschreibung müssen Sie zunächst einen Testzurückschreibungsjob ausführen und dann die entsprechenden MongoDB-Befehle ausführen.

Vorbereitende Schritte
Wenn die Authentifizierung aktiviert ist, müssen Sie Berechtigungsnachweise für Benutzer angeben, damit diese Berechtigungen für die Instanz in der Testzurückschreibungsoperation korrigieren können.

Informationen zu diesem Vorgang

Die Operation für differenzierte Zurückschreibung für MongoDB basiert auf einem Zurückschreibungsjob im Testmodus. Wenn Sie den Testzurückschreibungsjob in IBM Spectrum Protect Plus ausführen und die Befehle **mongodump** und **mongorestore** auf dem MongoDB-Server ausführen, können Sie auf einzelne Datenbanken oder Sammlungen aus der Wiederherstellungsquelle zugreifen.

Verwenden Sie die folgende Prozedur für die Ausführung einer der folgenden Tasks:

- Zurückschreibung einer beliebigen Anzahl Datenbanken mithilfe der Befehle **mongodump** und **mongorestore** für die für Sie erforderlichen Datenbanken
- Zurückschreibung einer beliebigen Anzahl Sammlungen mithilfe der Befehle **mongodump** und **mongorestore** für die für Sie erforderlichen Sammlungen

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **MongoDB**.
2. Klicken Sie auf **Zurückschreibungsjob erstellen**, um den Zurückschreibungsassistenten zu öffnen. MongoDB wird automatisch ausgewählt.
3. Führen Sie auf der Seite **Quellenauswahl** die folgenden Schritte aus:
   a) Klicken Sie in der Liste auf eine Quelle, um die Datenbanken anzuzeigen, die für Zurückschreibungsoperationen verfügbar sind. Sie können auch die Suchfunktion verwenden, um nach verfügbaren Instanzen zu suchen, und mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen wechseln.
   b) Klicken Sie auf das Symbol  neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll. Sie können mehrere Datenbanken aus der Liste auswählen.

      Die ausgewählten Quellen werden der Zurückschreibungsliste neben der Datenbankliste hinzugefügt. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Symbol  neben dem Eintrag.
   c) Klicken Sie auf **Weiter**, um fortzufahren.
4. Wählen Sie auf der Seite **Ziel definieren In alternative Instanz zurückschreiben** aus und wählen Sie die Zielinstanz aus, in die die Daten zurückgeschrieben werden sollen.

   Sie können die ursprüngliche Instanz nicht auswählen, da Sie die ursprünglichen Daten nicht überschreiben können, wenn Sie **In alternative Instanz zurückschreiben** auswählen. Instanzen mit verschiedenen Versionsständen können nicht ausgewählt werden. Andere Instanzen, die sich auf demselben Host wie die ursprüngliche Instanz befinden, können ebenfalls nicht ausgewählt werden.

   Klicken Sie auf **Weiter**, um fortzufahren.
5. Wählen Sie auf der Seite **Zurückschreibungsmethode** die Option **Test** aus und klicken Sie auf **Weiter**, um den Testzurückschreibungsprozess fortzusetzen.
6. Durchlaufen Sie die Seiten des Zurückschreibungsassistenten und wählen Sie die erforderlichen Optionen aus.
7. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs.

   Achtung: Überprüfen Sie die ausgewählten Optionen, bevor Sie mit **Übergeben** fortfahren, da Daten überschrieben werden, wenn die Anwendungsoption **Vorhandene Daten überschreiben** ausgewählt ist. Sie können einen Zurückschreibungsjob abbrechen, wenn er in Bearbeitung ist. Wenn die Option **Vorhandene Daten überschreiben** ausgewählt ist, werden Daten jedoch auch dann überschrieben, wenn Sie den Job abbrechen.
8. Melden Sie sich bei dem MongoDB-Server an, an den der Testzurückschreibungsjob gerichtet ist.
9. Führen Sie den MongoDB-Systembefehl `ps -ef | grep mongod` aus, um die Position der temporären MongoDB-Wiederherstellungsinstanz zu finden.
10. Führen Sie den MongoDB-Befehl `mongodump` aus, um eine Speicherauszugsdatei für jede einzelne Datenbank oder Sammlung zu erstellen.

Verwenden Sie den entsprechenden Befehl. Der erste Befehl gilt für eine Datenbank, der zweite Befehl für eine Sammlung:

```
mongodump --host <Hostname> --port <Port> --db <Datenbankname> <Speicherauszugsordner>
```

oder

```
mongodump --host <Hostname> --port <Port> --collection <Name_der_Sammlung> <Speicherauszugsordner>
```

11. Führen Sie den Befehl **mongorestore** aus, um die Speicherauszugsdatei in eine MongoDB-Instanz zurückzuschreiben. Wählen Sie entweder die ursprüngliche MongoDB-Instanz aus, für die die Sicherung erstellt wurde, oder wählen Sie eine beliebige alternative Instanz aus.

    Verwenden Sie den entsprechenden Befehl. Der erste Befehl gilt für eine Datenbank, der zweite Befehl für eine Sammlung:

    ```
    mongorestore --host <Hostname> --port <Port> --db <Datenbankname> <Speicherauszugsordner>\<Datenbankname>
    ```

    oder

    ```
    mongorestore --host <Hostname> --port <Port> --collection <Name_der_Sammlung> <Speicherauszugsordner>\<Datenbankname>
    ```

12. Wenn die Zurückschreibungsoperation für die Datenbank oder Sammlung beendet ist, rufen Sie **Jobs und Operationen** > **Aktive Ressourcen** auf.
13. Klicken Sie auf **Aktionen** > **Zurückschreibung abbrechen**, um die Prozedur für differenzierte Zurückschreibung zu beenden.

SQL Server-Daten sichern und zurückschreiben

Damit Inhalt auf einem SQL Server-Server geschützt werden kann, müssen Sie zunächst die SQL Server-Instanz registrieren, damit sie von IBM Spectrum Protect Plus erkannt wird. Erstellen Sie dann Jobs für Sicherungs- und Zurückschreibungsoperationen.

Systemanforderungen

Stellen Sie sicher, dass Ihre SQL Server-Umgebung die in „Microsoft SQL Server-Anforderungen” auf Seite 41 beschriebenen Systemanforderungen erfüllt.

Registrierung und Authentifizierung

Registrieren Sie jeden SQL Server-Server nach Namen oder nach IP-Adresse in IBM Spectrum Protect Plus. Wenn Sie einen SQL Server-Clusterknoten (AlwaysOn) registrieren, ist jeder Knoten nach Namen oder nach IP-Adresse zu registrieren. Beachten Sie, dass die IP-Adressen öffentlich und an Port 5985 empfangsbereit sein müssen. Der vollständig qualifizierte Domänenname und der DNS-Name des VM-Knotens müssen von der IBM Spectrum Protect Plus-Appliance aufgelöst und weitergeleitet werden können.

Die Benutzeridentität muss über die erforderlichen Berechtigungen zum Installieren und Starten des IBM Spectrum Protect Plus-Tools-Service auf dem Knoten verfügen, einschließlich der Berechtigung **Als Service anmelden**. Weitere Informationen zu dieser Berechtigung finden Sie in Add the Log on as a service Right to an Account.

In der Standardsicherheitsrichtlinie wird das Windows-NTLM-Protokoll verwendet und das Format der Benutzeridentität entspricht dem Standardformat *Domäne**Name*.

Wenn Sie Windows-Gruppenrichtlinienobjekte (GPO = Group Policy Object) verwenden, muss die GPO-Einstellung **Netzwerksicherheit: LAN Manager-Authentifizierungsebene** korrekt angegeben sein. Geben Sie sie mit einer der folgenden Optionen an:

- Nicht definiert
- Nur NTLMv2-Antworten senden
- Nur NTLMv2-Antworten senden \ LM ablehnen
- Nur NTLMv2-Antworten senden \ LM & NTLM ablehnen

Kerberos-Anforderungen

Die Kerberos-basierte Authentifizierung kann über eine Konfigurationsdatei in der IBM Spectrum Protect Plus-Appliance aktiviert werden. Dadurch wird das Standard-Windows-NTLM-Protokoll außer Kraft gesetzt.

Nur für die Kerberos-basierte Authentifizierung muss die Benutzeridentität im Format Benutzername@FQDN angegeben werden. Der Benutzername muss sich mit dem registrierten Kennwort authentifizieren können, um ein Ticket-Granting-Ticket (TGT) vom Key-Distribution-Center (KDC) in der Domäne anzufordern, die mit dem vollständig qualifizierten Domänennamen (FQDN) angegeben wird.

Für die Kerberos-Authentifizierung muss außerdem die Zeitabweichung zwischen dem Domänencontroller und der IBM Spectrum Protect Plus-Appliance weniger als fünf Minuten betragen.

Das Standard-Windows-NTLM-Protokoll ist nicht zeitabhängig.

Berechtigungen

Auf dem SQL Server-Server müssen im Systemanmeldeberechtigungsnachweis die Berechtigungen "public" und "sysadmin" aktiviert sein und darüber hinaus die Berechtigung für den Zugriff auf Clusterressourcen in einer SQL Server AlwaysOn-Umgebung. Wird ein einziger Benutzeraccount für alle SQL Server-Funktionen verwendet, muss für den SQL Server-Server eine Windows-Anmeldung mit den Berechtigungen "public" und "sysadmin" aktiviert werden.

In jeder SQL Server-Instanz kann ein spezifischer Benutzeraccount für den Zugriff auf die Ressourcen der betreffenden Instanz verwendet werden.

Zur Ausführung von Protokollsicherungsoperationen muss für den bei IBM Spectrum Protect Plus registrierten SQL Server-Benutzer die Berechtigung "sysadmin" aktiviert sein, um SQL Server-Agentenjobs verwalten zu können.

Der Windows-Taskplaner wird zum Planen von Protokollsicherungen verwendet. Abhängig von der Umgebung empfangen Benutzer unter Umständen den folgenden Fehler: `Eine angegebene Anmeldesitzung ist nicht vorhanden. Sie wurde gegebenenfalls bereits beendet.` Ursache hierfür ist eine Netzzugriffsgruppenrichtlinieneinstellung, die inaktiviert werden muss. Weitere Informationen zum Inaktivieren dieses Gruppenrichtlinienobjekts (GPO) enthält der folgende Microsoft Support-Artikel: https://support.microsoft.com/en-us/help/968264/error-message-when-you-try-to-map-to-a-network-drive-of-a-dfs-share-by.

SQL Server-Anwendungsserver hinzufügen

Wenn ein SQL Server-Anwendungsserver hinzugefügt wird, wird ein Bestand der Instanzen und Datenbanken, die dem Anwendungsserver zugeordnet sind, erfasst und zu IBM Spectrum Protect Plus hinzugefügt. Dieser Prozess ermöglicht es Ihnen, Sicherungs- und Zurückschreibungsjobs auszuführen und Berichte zu erstellen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen SQL Server-Host hinzuzufügen.

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **SQL** > **Sicherung**.
2. Klicken Sie auf **Anwendungsserver verwalten**.
3. Klicken Sie auf **Anwendungsserver hinzufügen**.
4. Füllen Sie die Felder im Fenster **Anwendungseigenschaften** aus:

   Hostadresse

Geben Sie die auflösbare IP-Adresse oder einen auflösbaren Pfad und Maschinennamen ein.

Vorhandenen Benutzer verwenden

Aktivieren Sie dieses Feld, um einen zuvor eingegebenen Benutzernamen und ein zuvor eingegebenes Kennwort für den Provider auszuwählen.

Benutzer-ID

Geben Sie Ihren Benutzernamen für den Provider ein. Die Benutzeridentität folgt dem Standardformat *Domäne**Name*, wenn die virtuelle Maschine einer Domäne zugeordnet ist. Das Format *lokaler_Administrator* wird verwendet, wenn der Benutzer ein lokaler Administrator ist.

Nur für die Kerberos-basierte Authentifizierung muss die Benutzeridentität im Format Benutzername@FQDN angegeben werden. Der Benutzername muss sich mit dem registrierten Kennwort authentifizieren können, um ein Ticket-Granting-Ticket (TGT) vom Key-Distribution-Center (KDC) in der Domäne anzufordern, die mit dem vollständig qualifizierten Domänennamen (FQDN) angegeben wird.

Kennwort

Geben Sie Ihr Kennwort für den Provider ein.

Maximale Anzahl gleichzeitig verwendeter Datenbanken

Definieren Sie die maximale Anzahl der Datenbanken, die gleichzeitig auf dem Server gesichert werden. Die Serverleistung wird beeinflusst, wenn eine große Anzahl Datenbanken gleichzeitig gesichert wird, da jede Datenbank mehrere Threads verwendet und Bandbreite verbraucht, wenn Daten kopiert werden. Verwenden Sie diese Option, um die Auswirkungen auf Serverressourcen zu steuern und die Auswirkungen auf den Produktionsbetrieb zu minimieren.

5. Klicken Sie auf **Speichern**. IBM Spectrum Protect Plus bestätigt eine Netzverbindung, fügt den Anwendungsserver zur IBM Spectrum Protect Plus-Datenbank hinzu und katalogisiert dann die Instanz.

   Wird eine Nachricht angezeigt, die angibt, dass die Verbindung nicht erfolgreich ist, überprüfen Sie Ihre Eingaben. Sind Ihre Eingaben korrekt und ist die Verbindung nicht erfolgreich, bitten Sie einen Systemadministrator, die Verbindungen zu überprüfen.

Nächste Schritte

Führen Sie die folgende Aktion aus, nachdem Sie den SQL Server-Anwendungsserver hinzugefügt haben:

Aktion	Vorgehensweise
Fügen Sie dem Anwendungsserver Benutzerberechtigungen hinzu.	Siehe „Rolle erstellen” auf Seite 317.

Zugehörige Konzepte

„Benutzerzugriff verwalten” auf Seite 311
Sie können mithilfe der rollenbasierten Zugriffssteuerung die Ressourcen und Berechtigungen festlegen, die IBM Spectrum Protect Plus-Benutzeraccounts zur Verfügung stehen.

Zugehörige Tasks

„SQL Server-Daten sichern” auf Seite 235
Verwenden Sie einen Sicherungsjob, um SQL Server-Umgebungen mit Momentaufnahmen zu sichern.

„SQL Server-Daten zurückschreiben” auf Seite 239
Verwenden Sie einen Zurückschreibungsjob, um eine Microsoft SQL Server-Umgebung aus Momentaufnahmen zurückzuschreiben. Nach der Ausführung von IBM Spectrum Protect Plus Instant Disk Restore-Jobs können Ihre SQL Server-Klone sofort verwendet werden. IBM Spectrum Protect Plus katalogisiert und überwacht alle geklonten Instanzen.

SQL Server-Ressourcen erkennen

SQL Server-Ressourcen werden automatisch erkannt, nachdem der Anwendungsserver IBM Spectrum Protect Plus hinzugefügt wurde. Sie können jedoch einen Bestandsjob ausführen, um alle Änderungen zu finden, die seit dem Hinzufügen des Anwendungsservers aufgetreten sind.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Bestandsjob auszuführen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **SQL** > **Sicherung**.
2. Wählen Sie in der Liste der SQL Server-Instanzen eine Instanz aus oder klicken Sie auf den Link für die Instanz, um zu der gewünschten Ressource zu navigieren. Wenn beispielsweise ein Bestandsjob für eine einzelne Datenbank in der Instanz ausgeführt werden soll, klicken Sie auf den Instanzlink und wählen Sie dann eine virtuelle Maschine aus.
3. Klicken Sie auf **Bestandsverarbeitung ausführen**.

Verbindung zu einem SQL Server-Anwendungsserver testen

Sie können die Verbindung zu einem SQL Server-Host testen. Die Testfunktion verifiziert die Kommunikation mit dem Host testet DNS-Einstellungen zwischen der virtuellen IBM Spectrum Protect-Appliance und dem Host.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Verbindung zu testen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **SQL** > **Sicherung**.
2. Klicken Sie auf **Anwendungsserver verwalten**.
3. Klicken Sie in der Liste der Hosts im Menü **Aktionen** für den Host auf **Testen**.

SQL Server-Daten sichern

Verwenden Sie einen Sicherungsjob, um SQL Server-Umgebungen mit Momentaufnahmen zu sichern.

Vorbereitende Schritte

Während der anfänglichen Basissicherung erstellt IBM Spectrum Protect Plus einen neuen vSnap-Datenträger und erstellt eine NFS-Freigabe. Bei Teilsicherungen wird der zuvor erstellte Datenträger wiederverwendet. Der IBM Spectrum Protect Plus-Agent stellt die Freigabe auf dem SQL Server-Server bereit, auf dem die Sicherung ausgeführt werden soll.

Wenn die Sicherung abgeschlossen ist, hebt der IBM Spectrum Protect Plus-Agent die Bereitstellung der Freigabe auf dem SQL Server-Server auf und erstellt eine vSnap-Momentaufnahme des Sicherungsdatenträgers.

Beachten Sie die folgenden Informationen:

- Bevor ein IBM Spectrum Protect Plus-Benutzer Sicherungs- und Zurückschreibungsoperationen implementieren kann, müssen dem Benutzer Rollen und Ressourcengruppen zugeordnet werden. Erteilen Sie Benutzern mithilfe des Fensters **Accounts** Zugriff auf Ressourcen und Sicherungs- und Zurückschreibungsoperationen. Weitere Informationen finden Sie in Kapitel 13, „Benutzerzugriff verwalten”, auf Seite 311.
- Der Microsoft-iSCSI-Initiator muss aktiviert werden und auf dem Windows-Server ausgeführt werden. Eine iSCSI-Route muss zwischen dem SQL-System und dem vSnap-Server aktiviert werden. Weitere Informationen finden Sie in Microsoft iSCSI Initiator Step-by-Step Guide.
- Vermeiden Sie das Konfigurieren der Protokollsicherung für eine einzelne SQL-Datenbank mithilfe mehrerer Sicherungsjobs. Protokolle werden während der Protokollsicherungsoperationen abgeschnitten. Wenn eine einzelne SQL-Datenbank mehreren Jobdefinitionen mit aktivierter Protokollsicherung hinzugefügt wird, schneidet eine Protokollsicherung von einem Job ein Protokoll ab, bevor es vom nächsten Job gesichert wird. Dies kann zur Folge haben, dass Jobs für Zurückschreibungen nach Zeitpunkt fehlschlagen.
- IBM Spectrum Protect Plus unterstützt nicht die Protokollsicherung von einfachen Wiederherstellungsmodellen.
- Bevor Protokolle in vSnap kopiert werden, verwendet SPP den für die SQL Server-Instanz konfigurierten Sicherungsordner als Staging-Bereich zum Sammeln von Protokollen. Der Datenträger, auf dem sich dieser Ordner befindet, muss über genügend Speicherbereich verfügen, um alle Transaktionsprotokolle

zwischen Sicherungsjobs aufnehmen zu können. Der Staging-Bereich kann geändert werden, indem die Konfiguration des Sicherungsordners mithilfe von SQL Server Management Studio (SSMS) geändert wird.

- Failover einer SQL-Clusterinstanz während der Sicherung wird nicht unterstützt.
- Ist die Sicherung einer großen Anzahl Datenbanken geplant, müssen Sie möglicherweise die maximale Anzahl Worker-Threads auf jeder zugeordneten SQL Server-Instanz erhöhen, um sicherzustellen, dass Sicherungsjobs erfolgreich ausgeführt werden. Der Standardwert für die maximale Anzahl Worker-Threads ist 0. Der Server bestimmt automatisch den Wert für die maximale Anzahl Worker-Threads auf der Basis der Anzahl Prozessoren, die für den Server verfügbar sind. SQL Server verwendet die Threads aus diesem Pool für Netzverbindungen, Datenbankprüfpunkte und Abfragen. Außerdem erfordert eine Sicherung jeder Datenbank einen zusätzlichen Thread aus diesem Pool. Wenn ein Sicherungsjob eine große Anzahl Datenbanken einschließt, ist der Standardwert für die maximale Anzahl Worker-Threads möglicherweise nicht groß genug, um alle Datenbanken zu sichern. In diesem Fall schlägt der Job fehl. Weitere Informationen zum Vergrößern der Option für die maximale Anzahl Worker-Threads finden Sie in Konfigurieren der Serverkonfigurationsoption 'Maximale Anzahl von Arbeitsthreads'.
- Wenn eine Protokollsicherung einer sekundären SQL AlwaysOn-Datenbank mit dem folgenden Fehler fehlschlägt, muss die Sicherungsvorgabe der Verfügbarkeitsgruppe in "Primär" geändert werden:

  ```
  Protokollsicherung für Datenbank "Datenbankname" ist auf einem
  sekundären Replikat fehlgeschlagen, da ein Synchronisationspunkt für die
  primäre Datenbank nicht erstellt werden konnte.
  ```

  Wird die Vorgabe in "Primär" geändert, wird das Protokoll auf dem primären Replikat gesichert. Nach einer erfolgreichen Protokollsicherung des primären Replikats kann die Sicherungsvorgabe geändert werden.

Führen Sie die folgenden Aktionen aus:

- Registrieren Sie die Provider, die gesichert werden sollen. Weitere Informationen finden Sie in „SQL Server-Anwendungsserver hinzufügen” auf Seite 233.
- Konfigurieren Sie SLA-Richtlinien. Weitere Informationen finden Sie in „Sicherungsrichtlinien erstellen” auf Seite 75.
- Bevor SQL-Sicherungsjobs definiert und ausgeführt werden, müssen Sie die Einstellungen für den Spiegelkopiespeicher für die Datenträger konfigurieren, auf denen sich die SQL-Datenbanken befinden. Diese Einstellung wird einmal pro Datenträger konfiguriert. Werden dem Job neue Datenbanken hinzugefügt, muss die Einstellung für alle neuen Datenträger, die SQL-Datenbanken enthalten, konfiguriert werden. Klicken Sie im Windows Explorer mit der rechten Maustaste auf den Quellendatenträger und wählen Sie die Registerkarte **Spiegelkopien** aus. Setzen Sie **Maximale Größe** auf **Kein Grenzwert** oder auf eine angemessene Größe (abhängig von der Größe des Quellendatenträgers und den E/A-Aktivitäten) und klicken Sie dann auf **OK**. Der Spiegelkopiespeicherbereich muss sich zum Zeitpunkt der Sicherung auf demselben Datenträger oder auf einem anderen verfügbaren Datenträger befinden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen SQL-Sicherungsjob zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **SQL**.
2. Wählen Sie eine SQL Server-Instanz aus, die gesichert werden soll.

   Verwenden Sie die Suchfunktion, um nach verfügbaren Instanzen zu suchen, und wechseln Sie mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen. Die verfügbaren Optionen sind **Standalone-/Failover-Cluster** und **AlwaysOn**.
3. Klicken Sie auf **SLA-Richtlinie auswählen**, um eine oder mehrere SLA-Richtlinien, die Ihre Sicherungsdatenkriterien erfüllen, zur Jobdefinition hinzuzufügen.
4. Um die Jobdefinition mithilfe von Standardoptionen zu erstellen, klicken Sie auf **Speichern**.

   Der Job wird wie mit den von Ihnen ausgewählten SLA-Richtlinien definiert ausgeführt. Um den Job manuell auszuführen, klicken Sie auf **Jobs und Operationen** > **Zeitplan**. Wählen Sie den Job aus und klicken Sie auf **Aktionen** > **Starten**.

Tipp: Die Schaltfläche **Ausführen** ist nur für die Sicherung einer einzelnen Datenbank aktiviert; auf die Datenbank muss außerdem eine SLA-Richtlinie angewendet sein.

5. Um Optionen zu editieren, bevor die Jobdefinition erstellt wird, klicken Sie auf **Optionen auswählen**. Definieren Sie die Jobdefinitionsoptionen.

   Protokollsicherung aktivieren

   Wählen Sie diese Option aus, um es IBM Spectrum Protect Plus zu ermöglichen, Transaktionsprotokolle zu sichern und dann die zugrunde liegenden Platten zu schützen.

   IBM Spectrum Protect Plus schneidet nachfolgende Protokollsicherungen von Datenbanken, die gesichert werden, automatisch ab. Wenn Datenbankprotokolle nicht mit IBM Spectrum Protect Plus gesichert werden, werden Protokolle nicht von IBM Spectrum Protect Plus abgeschnitten, und müssen separat verwaltet werden.

   Wenn ein SQL-Sicherungsjob mit aktivierten Protokollsicherungen ausgeführt wird, werden alle Transaktionsprotokolle bis zu dem Job, der gerade ausgeführt wird, auf dem SQL Server-Server gelöscht. Das Löschen von Protokollen findet nur statt, wenn der SQL-Sicherungsjob erfolgreich ausgeführt wird. Werden Protokollsicherungen während einer erneuten Ausführung des Jobs inaktiviert, findet das Löschen von Protokollen nicht statt.

   Wird eine Quellendatenbank überschrieben, werden alle alten Transaktionsprotokolle bis zu diesem Punkt in ein Verzeichnis "Komprimieren" gestellt, sobald die Zurückschreibung der ursprünglichen Datenbank abgeschlossen ist. Wenn die nächste Ausführung des SQL-Sicherungsjobs abgeschlossen ist, wird der Inhalt des Ordners "Komprimieren" entfernt.

   Um Protokollsicherungen auszuführen, muss der Benutzer des SQL Server-Agentenservice ein lokaler Windows-Administrator sein und über die aktivierte Berechtigung "sysadmin" verfügen, um SQL Server-Agentenjobs zu verwalten. Der Agent verwendet diesen Administratoraccount, um Protokollsicherungsjobs zu aktivieren und auf Protokollsicherungsjobs zuzugreifen. Der Benutzer des IBM Spectrum Protect Plus SQL Server-Agentenservice muss außerdem mit dem SQL Server-Service- und SQL Server-Agentenservice-Account für jede SQL Server-Instanz übereinstimmen, die geschützt werden soll.

   SQL-Protokolldateien werden temporär in einem lokalen Bereitstellungsbereich gespeichert, bevor sie in eine CIFS-Freigabe kopiert werden. Das SQL Server-Standardsicherungsziel dient als Bereitstellungsbereich und muss über genügend freien Speicherbereich verfügen, um die Transaktionsprotokolldateien temporär zu speichern, bevor sie in die CIFS-Freigabe kopiert werden können.

   Um die Erstellung eines Protokollsicherungszeitplans für mehrere Datenbanken auf derselben SQL Server-Instanz zu ermöglichen, stellen Sie sicher, dass alle Datenbanken derselben SLA-Richtlinie hinzugefügt werden.

   Wird diese Option ausgewählt, sind Optionen für die Zurückschreibung nach Zeitpunkt für SQL-Zurückschreibungsoperationen verfügbar.

   Maximale Anzahl paralleler Datenströme pro Datenbank

   Definieren Sie die maximale Anzahl Datenströme pro Datenbank zum Sicherungsspeicher. Diese Einstellung gilt für jede Datenbank in der Jobdefinition. Mehrere Datenbanken können parallel gesichert werden, wenn der Wert der Option auf **1** gesetzt wird. Mehrere parallele Datenströme können die Sicherungsgeschwindigkeit verbessern, die Nutzung hoher Bandbreite kann sich jedoch auf die Systemgesamtleistung auswirken.

6. Wenn die jobspezifischen Informationen korrekt sind, klicken Sie auf **Speichern**.

   Der Job wird wie mit Ihrer SLA-Richtlinie definiert ausgeführt oder kann manuell mithilfe des Fensters "Jobüberwachung" ausgeführt werden.

7. Um zusätzliche Optionen zu konfigurieren, klicken Sie auf das Feld **Richtlinienoptionen**, das dem Job im Abschnitt **SLA-Richtliniestatus** zugeordnet ist. Definieren Sie die zusätzlichen Richtlinienoptionen:

   Vorscripts und Nachscripts

Führen Sie ein Vorscript oder Nachscript aus. Vorscripts und Nachscripts sind Scripts, die vor oder nach der Ausführung eines Jobs ausgeführt werden können. Batch- und PowerShell-Scripts werden unterstützt.

Wählen Sie im Abschnitt **Vorscript** oder **Nachscript** ein hochgeladenes Script und einen Anwendungs- oder Scriptserver aus, auf dem das Script ausgeführt wird. Um einen Anwendungsserver auszuwählen, auf dem das Script ausgeführt wird, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Scripts und Scriptserver werden auf der Seite **Systemkonfiguration** > **Script** konfiguriert.

Um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt, wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus.

Wenn diese Option aktiviert wird und ein Vorscript oder Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird versucht, die Sicherungs- oder Zurückschreibungsoperation auszuführen, und der Taskstatus für das Vorscript wird als ABGESCHLOSSEN zurückgemeldet. Wenn ein Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird der Taskstatus für das Nachscript als ABGESCHLOSSEN zurückgemeldet.

Wenn diese Option inaktiviert wird, wird nicht versucht, die Sicherung oder Zurückschreibung auszuführen, und der Taskstatus für das Vorscript oder Nachscript wird als FEHLGESCHLAGEN zurückgemeldet.

Ressourcen ausschließen

Schließen Sie bestimmte Ressourcen mit einzelnen oder mehreren Ausschlussmustern aus dem Sicherungsjob aus. Ressourcen können mit einer exakten Übereinstimmung oder mit Sternen als Platzhalterzeichen, die vor dem Muster (*test) oder hinter dem Muster (test*) angegeben werden, ausgeschlossen werden.

Mehrere Sterne als Platzhalterzeichen werden auch in einem einzelnen Muster unterstützt. Die Muster unterstützen alphanumerische Standardzeichen sowie die folgenden Sonderzeichen: - _ und *.

Trennen Sie mehrere Filter durch ein Semikolon voneinander.

Gesamtsicherung der Ressourcen erzwingen

Erzwingen Sie Basissicherungsoperationen für bestimmte virtuelle Maschinen oder Datenbanken in der Sicherungsjobdefinition. Trennen Sie mehrere Ressourcen durch ein Semikolon voneinander.

8. Um alle zusätzlichen Optionen zu speichern, die konfiguriert wurden, klicken Sie auf **Speichern**.

Nächste Schritte

Führen Sie die folgende Aktion aus, nachdem Sie die Sicherungsjobdefinition erstellt haben:

Aktion	Vorgehensweise
Erstellen Sie eine SQL-Zurückschreibungsjobdefinition.	Siehe „SQL Server-Daten zurückschreiben” auf Seite 239.

Zugehörige Konzepte

„Scripts für Sicherungs- und Zurückschreibungsoperationen konfigurieren” auf Seite 267
Vorscripts und Nachscripts sind Scripts, die ausgeführt werden können, bevor oder nachdem Sicherungs- und Zurückschreibungsjobs auf Jobebene ausgeführt werden. Unterstützt werden Shell-Scripts für Linux-basierte Systeme sowie Batch- und PowerShell-Scripts für Windows-basierte Systeme. Scripts werden lokal erstellt, über die Seite **Script** in Ihre Umgebung hochgeladen und dann auf Jobdefinitionen angewendet.

Zugehörige Tasks

„Jobs starten” auf Seite 264
Sie können einen Job selbst dann bedarfsgesteuert ausführen, wenn die Ausführung des Jobs gemäß einem Zeitplan festgelegt ist.

SQL Server-Daten zurückschreiben

Verwenden Sie einen Zurückschreibungsjob, um eine Microsoft SQL Server-Umgebung aus Momentaufnahmen zurückzuschreiben. Nach der Ausführung von IBM Spectrum Protect Plus Instant Disk Restore-Jobs können Ihre SQL Server-Klone sofort verwendet werden. IBM Spectrum Protect Plus katalogisiert und überwacht alle geklonten Instanzen.

Vorbereitende Schritte

Die folgenden Voraussetzungen müssen erfüllt sein:

- Erstellen Sie einen SQL-Sicherungsjob und führen Sie ihn aus. Anweisungen finden Sie in „SQL Server-Daten sichern" auf Seite 235.
- Bevor ein IBM Spectrum Protect Plus-Benutzer Daten zurückschreiben kann, müssen dem Benutzer die entsprechenden Rollen und Ressourcengruppen zugeordnet werden. Erteilen Sie Benutzern mithilfe des Fensters **Accounts** Zugriff auf Ressourcen und Sicherungs- und Zurückschreibungsoperationen. Anweisungen finden Sie in Kapitel 13, „Benutzerzugriff verwalten", auf Seite 311.
- Wenn Sie planen, eine Wiederherstellung nach Zeitpunkt auszuführen, stellen Sie sicher, dass der SQL-Zurückschreibungszielinstanzservice und der IBM Spectrum Protect Plus SQL Server-Service denselben Benutzeraccount verwenden.

Beachten Sie die folgenden Einschränkungen und Hinweise:

- Wenn Sie planen, eine Produktionszurückschreibungsoperation in einen SQL Server-Failover-Cluster auszuführen, muss der Stammdatenträger des alternativen Dateipfads für Hostdatenbank- und Protokolldateien auswählbar sein. Der Datenträger sollte zur SQL Server-Zielcluster-Serverressourcengruppe gehören und eine Abhängigkeit des SQL Server-Cluster-Servers darstellen.
- Eine Zurückschreibung von Daten auf einen komprimierten NTFS- oder FAT-Datenträger ist aufgrund von SQL Server-Datenbankeinschränkungen nicht möglich. Weitere Informationen finden Sie in Description of support for SQL Server databases on compressed volumes.
- Wenn Sie planen, Daten an eine alternative Position zurückzuschreiben, muss für das SQL Server-Ziel dieselbe Version von SQL Server oder eine höhere Version ausgeführt werden. Weitere Informationen finden Sie in Kompatibilitätsunterstützung.
- Wenn Sie Daten in eine primäre Instanz in einer Umgebung mit SQL AlwaysOn-Verfügbarkeitsgruppen zurückschreiben, wird die Datenbank der AlwaysOn-Zieldatenbankgruppe hinzugefügt. Nach der primären Zurückschreibungsoperation wird für die sekundäre Datenbank vom SQL-Server in Umgebungen, in denen automatisches Seeding unterstützt wird (Microsoft SQL Server 2016 und höher), ein Seeding ausgeführt. Die Datenbank wird dann in der Zielverfügbarkeitsgruppe aktiviert. Die Synchronisationszeit hängt vom übertragenen Datenvolumen und der Verbindung zwischen den primären und sekundären Replikaten ab.

  Wenn automatisches Seeding nicht unterstützt wird oder nicht aktiviert ist, muss eine sekundäre Zurückschreibung von dem Zurückschreibungspunkt mit dem geringsten LSN-Abstimmungsverlust der primären Instanz ausgeführt werden. Protokollsicherungen mit dem letzten PIT-Zurückschreibungspunkt, der von IBM Spectrum Protect Plus erstellt wurde, müssen zurückgeschrieben werden, wenn die Protokollsicherung auf der primären Instanz aktiviert wurde. Die Zurückschreibungsoperation für die sekundäre Datenbank wird im Status RESTORING (Zurückschreibungsstatus) ausgeführt und Sie müssen den Befehl **T-SQL** ausgeben, um die Datenbank der Zielgruppe hinzuzufügen. Weitere Informationen finden Sie in Transact-SQL-Referenz (Datenbank-Engine).
- Bei einer Zurückschreibung aus einem IBM Spectrum Protect-Archiv werden Dateien vom Band in einen Staging-Pool migriert, bevor der Job gestartet wird. Abhängig von der Größe der Zurückschreibung kann dieser Prozess mehrere Stunden dauern.

Informationen zu diesem Vorgang

Instant Disk Restore verwendet das iSCSI-Protokoll für die sofortige Bereitstellung von LUNs ohne die Übertragung von Daten. Datenbanken, für die Momentaufnahmen erstellt wurden, werden katalogisiert und sind sofort ohne physische Datenübertragung wiederherstellbar.

Die folgenden Zurückschreibungsmodi werden unterstützt:

Instant Access-Modus
Im Instant Access-Modus wird keine weitere Aktion ausgeführt, nachdem die Freigabe bereitgestellt wurde. Benutzer können jede angepasste Wiederherstellung mithilfe der Dateien auf dem vSnap-Datenträger ausführen. Eine Instant Access-Zurückschreibung einer AlwaysOn-Datenbank wird in die lokale Zielinstanz zurückgeschrieben.

Testmodus
Im Testmodus erstellt der Agent eine neue Datenbank, indem er die Datendateien direkt vom vSnap-Datenträger verwendet.

Produktionsmodus
Im Produktionsmodus schreibt der Agent zunächst die Dateien vom vSnap-Datenträger in den primären Speicher zurück und erstellt dann unter Verwendung der zurückgeschriebenen Dateien die neue Datenbank.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen SQL-Zurückschreibungsjob zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **SQL** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch öffnen, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **SQL** klicken.
   - Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Informationssymbol im Navigationsfenster des Assistenten.
   - Um die optionalen Seiten im Assistenten zu übergehen, wählen Sie **Optionale Schritte überspringen** aus.

2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Aktionen aus:
   a) Klicken Sie in der Liste auf eine Quelle, um die Datenbanken anzuzeigen, die für Zurückschreibungsoperationen verfügbar sind. Mithilfe des Filters **Sicht** können Sie zwischen den angezeigten Quellen wechseln, um entweder SQL Server-Instanzen in einer Standalone- oder Clusterumgebung oder AlwaysOn-Verfügbarkeitsgruppen anzuzeigen.

      Sie können auch die Suchfunktion verwenden, um in den Instanzen oder Verfügbarkeitsgruppen nach Datenbanken zu suchen.

   b) Klicken Sie auf das Plussymbol neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll. Sie können mehrere Datenbanken aus der Liste auswählen.

      Die ausgewählten Quellen werden der Zurückschreibungsliste neben der Datenbankliste hinzugefügt. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Minussymbol neben dem Eintrag.

   c) Klicken Sie auf **Weiter**, um fortzufahren.

3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der Datenbank an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren. Einige Felder werden erst angezeigt, nachdem ein zugehöriges Feld ausgewählt wurde.

Option	Beschreibung
Zurückschreibungstyp	Wählen Sie den Typ des Zurückschreibungsjobs aus: **Bedarfsgesteuert: Momentaufnahme** Führt einen einmaligen Zurückschreibungsjob aus einer Datenbankmomentaufnahme aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten.

Option	Beschreibung
	Bedarfsgesteuert: Zeitpunkt Führt einen einmaligen Zurückschreibungsjob aus einer Sicherung einer Datenbank nach Zeitpunkt aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Wiederholt auftretend** Erstellt einen sich wiederholenden Job für die Zurückschreibung nach Zeitpunkt, der gemäß einem Zeitplan ausgeführt wird.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position aus, von der Daten zurückgeschrieben werden sollen: **Site** Die Site, an der Momentaufnahmen gesichert wurden. Die Site wird im Fenster **Systemkonfiguration** > **Site** definiert. **Cloudauslagerung** Der Cloud-Server, auf den Momentaufnahmen ausgelagert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Auslagerung** Der Repository-Server, auf den Momentaufnahmen ausgelagert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert. **Cloudarchivierung** Der Cloud-Server, auf dem Momentaufnahmen archiviert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Archivierung** Der Repository-Server, auf dem Momentaufnahmen archiviert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus: **Demo** Die Demonstrationssite, von der Momentaufnahmen zurückgeschrieben werden sollen. **Primär** Die primäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. **Sekundär** Die sekundäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, wählen Sie einen Server im Menü **Position auswählen** aus.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Zurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Zurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datenbereich aus.

Option	Beschreibung
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wenn Sie Daten aus einer Cloudressource oder von einem Repository-Server zurückschreiben, wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben; wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert oder in einer Cloudressource oder auf einem Repository-Server archiviert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway auswählen.

4. Geben Sie auf der Seite **Ziel definieren** an, wohin die Datenbank zurückgeschrieben werden soll, und klicken Sie auf **Weiter**.

   In ursprüngliche Instanz zurückschreiben
   Wählen Sie diese Option aus, um die Datenbank in die ursprüngliche Instanz zurückzuschreiben.

   In primäre Instanz zurückschreiben
   Wählen Sie für Zurückschreibungsoperationen in einer SQL AlwaysOn-Umgebung diese Option aus, um die Datenbank in die primäre Instanz der AlwaysOn-Verfügbarkeitsgruppe zurückzuschreiben. Die Datenbank wird der Gruppe wieder hinzugefügt.

   In alternative Instanz zurückschreiben
   Wählen Sie diese Option aus, um die Datenbank an ein lokales Ziel zurückzuschreiben, das nicht mit der ursprünglichen Instanz übereinstimmt; wählen Sie dann die alternative Position aus der Liste der verfügbaren Server aus.

   Bei Zurückschreibungsoperationen in einer SQL AlwaysOn-Umgebung im Testmodus wird die Verfügbarkeitsquellendatenbank in die ausgewählte Zielinstanz zurückgeschrieben.

   Bei Zurückschreibungsoperationen in einer SQL AlwaysOn-Umgebung im Produktionsmodus wird die zurückgeschriebene Datenbank der Zielverfügbarkeitsgruppe hinzugefügt, wenn die Zielinstanz ein primäres Replikat ist. Wenn die Zielinstanz ein sekundäres Replikat der Zielverfügbarkeitsgruppe ist, wird die Datenbank in das sekundäre Replikat zurückgeschrieben und die Datenbank verbleibt im Zurückschreibungsstatus.

   Wenn die Option für automatisches Seeding für die Zielverfügbarkeitsgruppe aktiviert ist, werden die Dateipfade der sekundären Datenbank mit denen der primären Datenbank synchronisiert. Wenn das Protokoll der primären Datenbank nicht abgeschnitten wird, kann die sekundäre Datenbank von SQL der Verfügbarkeitsgruppe hinzugefügt werden.

5. Definieren Sie auf der Seite **Zurückschreibungsmethode** den Zurückschreibungsjob, der standardmäßig im Test-, Produktions- oder Instant Access-Modus ausgeführt werden soll.

   Für den Test- oder Produktionsmodus können Sie wahlweise einen neuen Namen für die zurückgeschriebene Datenbank eingeben.

   Für den Produktionsmodus können Sie außerdem einen neuen Ordner für die zurückgeschriebene Datenbank angeben, indem Sie die Datenbank erweitern und einen neuen Ordnernamen eingeben.

   Klicken Sie auf **Weiter**, um fortzufahren.

   Nachdem der Job erstellt wurde, kann er im Test-, Produktions- oder Instant Access-Modus im Fenster **Jobsitzungen** ausgeführt werden.

6. Konfigurieren Sie auf der Seite **Joboptionen** weitere Optionen für den Zurückschreibungsjob und klicken Sie auf **Weiter**, um fortzufahren.

   Wiederherstellungsoptionen
   Definieren Sie die folgenden Optionen für die Wiederherstellung nach Zeitpunkt:

Keine Wiederherstellung
Versetzen Sie die ausgewählte Datenbank in den Status RESTORING (Zurückschreibungsstatus). Wenn Sie Transaktionsprotokollsicherungen ohne IBM Spectrum Protect Plus verwalten, können Sie Protokolldateien manuell zurückschreiben und die Datenbank einer Verfügbarkeitsgruppe hinzufügen, vorausgesetzt, die LSN der sekundären und primären Datenbankkopien erfüllt die Kriterien.

Einschränkung: Die Option **Keine Wiederherstellung** unterstützt keine Zurückschreibungsoperationen im Produktionsmodus in SQL AlwaysOn-Gruppen.

Bis zum Ende der Sicherung wiederherstellen
Mit dieser Option wird die ausgewählte Datenbank mit dem Status zum Zeitpunkt der Erstellung der Sicherung zurückgeschrieben.

Bis zu einem bestimmten Zeitpunkt wiederherstellen
Wenn die Protokollsicherung mithilfe einer SQL-Sicherungsjobdefinition aktiviert wird, sind Optionen für die Zurückschreibung nach Zeitpunkt verfügbar, wenn eine SQL-Zurückschreibungsjobdefinition erstellt wird. Wählen Sie eine der folgenden Optionen aus:

- **Nach Zeit**. Wählen Sie diese Option aus, um eine Wiederherstellung nach Zeitpunkt anhand eines bestimmten Datums und einer bestimmten Uhrzeit zu konfigurieren.
- **Nach Transaktions-ID**. Wählen Sie diese Option aus, um eine Wiederherstellung nach Zeitpunkt nach Transaktions-ID zu konfigurieren.

In einer eigenständigen Zurückschreibungsoperation sucht IBM Spectrum Protect Plus die Zurückschreibungspunkte unmittelbar vor und nach dem ausgewählten Zeitpunkt. Während der Wiederherstellung werden der ältere Datensicherungsdatenträger und der neuere Protokollsicherungsdatenträger bereitgestellt. Wenn der Zeitpunkt nach der letzten Sicherungsoperation liegt, wird ein temporärer Zurückschreibungspunkt erstellt.

Wenn Sie Zurückschreibungsoperationen in einer SQL AlwaysOn-Umgebung im Testmodus ausführen, wird die zurückgeschriebene Datenbank in die Instanz eingebunden, in der sich die Verfügbarkeitsgruppe befindet.

Wenn Sie Zurückschreibungsoperationen in einer SQL AlwaysOn-Umgebung im Produktionsmodus ausführen, wird die zurückgeschriebene primäre Datenbank mit der Verfügbarkeitsgruppe verknüpft. Wenn die Option für automatisches Seeding für die Zielverfügbarkeitsgruppe aktiviert ist, werden die Dateipfade der sekundären Datenbank mit denen der primären Datenbank synchronisiert. Wenn das Protokoll der primären Datenbank nicht abgeschnitten wird, kann die sekundäre Datenbank von SQL der Verfügbarkeitsgruppe hinzugefügt werden.

Anwendungsoptionen
Definieren Sie die Anwendungsoptionen:

Vorhandene Datenbanken überschreiben
Ermöglichen Sie dem Zurückschreibungsjob das Überschreiben der ausgewählten Datenbank. Standardmäßig ist diese Option nicht aktiviert.

Tipp: Bevor Sie Zurückschreibungsoperationen in einer SQL AlwaysOn-Umgebung mithilfe des Produktionsmodus und mit der Option **Vorhandene Datenbanken überschreiben** ausführen, stellen Sie sicher, dass die Datenbank nicht auf den Replikaten der Zielverfügbarkeitsgruppe vorhanden ist. Dazu müssen Sie die ursprünglichen Datenbanken (die überschrieben werden sollen) manuell auf allen Replikaten der Zielverfügbarkeitsgruppe löschen.

Maximale Anzahl paralleler Datenströme pro Datenbank
Definieren Sie die maximale Anzahl Datenströme pro Datenbank aus dem Sicherungsspeicher. Diese Einstellung gilt für jede Datenbank in der Jobdefinition. Mehrere Datenbanken können auch dann parallel zurückgeschrieben werden, wenn der Wert der Option auf 1 gesetzt wird. Mehrere parallele Datenströme können die Zurückschreibungsgeschwindigkeit verbessern, die Nutzung hoher Bandbreite kann sich jedoch auf die Systemgesamtleistung auswirken.

Diese Option ist nur gültig, wenn Sie eine SQL Server-Datenbank mit ihrem ursprünglichen Datenbanknamen an die ursprüngliche Position zurückschreiben.

Erweiterte Optionen
Definieren Sie die erweiterten Jobdefinitionsoptionen:

Bereinigung direkt beim Fehlschlagen des Jobs ausführen
Zugeordnete Ressourcen werden automatisch im Rahmen einer Zurückschreibungsoperation bereinigt, wenn die Wiederherstellung fehlschlägt.

Sitzungsüberschreibung zulassen
Wählen Sie diese Option aus, um eine vorhandene Datenbank während der Wiederherstellung durch eine Datenbank mit demselben Namen zu ersetzen. Wenn eine Instant Disk Restore-Operation für eine Datenbank ausgeführt wird und eine andere Datenbank mit demselben Namen bereits auf dem Zielhost oder -cluster ausgeführt wird, fährt IBM Spectrum Protect Plus die vorhandene Datenbank herunter, bevor die wiederhergestellte Datenbank gestartet wird. Wenn diese Option nicht ausgewählt wird, schlägt der Zurückschreibungsjob fehl, wenn IBM Spectrum Protect Plus eine vorhandene aktive Datenbank mit demselben Namen findet.

Mit Zurückschreibungen der anderen ausgewählten Datenbanken fortfahren, auch wenn eine Zurückschreibung fehlschlägt
Aktivieren Sie diese Option, um mit der Wiederherstellung einer Ressource in einer Serie fortzufahren, wenn die Wiederherstellung der vorherigen Ressource fehlschlägt. Wenn diese Option nicht aktiviert wird, wird der Zurückschreibungsjob gestoppt, wenn die Wiederherstellung einer Ressource fehlschlägt.

Protokollpriorität (nur Instant Access)
Sind mehrere Speicherprotokolle verfügbar, wählen Sie das Protokoll aus, das in dem Job Priorität haben soll. Die verfügbaren Protokolle sind **iSCSI** und **Fibre Channel**.

Mountpunktpräfix
Geben Sie für Instant Access-Zurückschreibungsoperationen das Präfix für den Pfad an, für den der Mountpunkt bereitgestellt werden soll.

7. Optional: Geben Sie auf der Seite **Scripts anwenden** Scripts an, die vor oder nach der Ausführung einer Operation auf Jobebene ausgeführt werden können. Batch- und PowerShell-Scripts werden unterstützt.

Vorscript
Wählen Sie dieses Kontrollkästchen aus, um ein hochgeladenes Script und einen Anwendungs- oder Scriptserver auszuwählen, auf dem das Vorscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, auf dem das Vorscript ausgeführt wird, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Scripts und Scriptserver werden auf der Seite **Systemkonfiguration** > **Script** konfiguriert.

Nachscript
Wählen Sie diese Option aus, um ein hochgeladenes Script und einen Anwendungs- oder Scriptserver auszuwählen, auf dem das Nachscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, auf dem das Nachscript ausgeführt wird, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Scripts und Scriptserver werden auf der Seite **Systemkonfiguration** > **Script** konfiguriert.

Job/Task bei Scriptfehler fortsetzen
Wählen Sie dieses Kontrollkästchen aus, um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt.

Wenn Sie dieses Kontrollkästchen auswählen und ein Vorscript oder Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird versucht, die Sicherungs- oder Zurückschreibungsoperation auszuführen, und der Taskstatus für das Vorscript wird als ABGESCHLOSSEN zurückgemeldet. Wenn ein Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird der Taskstatus für das Nachscript als ABGESCHLOSSEN zurückgemeldet.

Wenn Sie dieses Kontrollkästchen abwählen, wird nicht versucht, die Sicherungs- oder Zurückschreibungsoperation auszuführen, und der Taskstatus für das Vorscript oder Nachscript wird als FEHLGESCHLAGEN zurückgemeldet.

8. Führen Sie auf der Seite **Zeitplan** eine der folgenden Aktionen aus:

- Wenn Sie einen bedarfsgesteuerten Job ausführen, klicken Sie auf **Weiter**.

- Wenn Sie einen sich wiederholenden Job definieren, geben Sie einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an. Klicken Sie auf **Weiter**.

9. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs und klicken Sie auf **Übergeben**, um den Job zu erstellen.

Ergebnisse

Ein bedarfsgesteuerter Job startet, nachdem Sie auf **Übergeben** geklickt haben, und der Satz **Bedarfsgesteuerte Zurückschreibung** wird dem Fenster **Jobsitzungen** kurz danach hinzugefügt. Um den Fortschritt der Zurückschreibungsoperation anzuzeigen, erweitern Sie den Job. Sie können die Protokolldatei auch herunterladen, indem Sie auf das Symbol für Herunterladen  klicken.

Ein sich wiederholender Job startet zum geplanten Startzeitpunkt, wenn Sie den Zeitplan auf der Seite **Jobs und Operationen** > **Zeitplan** starten.

Alle aktiven Jobs sind auf der Seite **Jobs und Operationen** > **Aktive Jobs** anzeigbar.

Zugehörige Konzepte

„Scripts für Sicherungs- und Zurückschreibungsoperationen konfigurieren” auf Seite 267
Vorscripts und Nachscripts sind Scripts, die ausgeführt werden können, bevor oder nachdem Sicherungs- und Zurückschreibungsjobs auf Jobebene ausgeführt werden. Unterstützt werden Shell-Scripts für Linux-basierte Systeme sowie Batch- und PowerShell-Scripts für Windows-basierte Systeme. Scripts werden lokal erstellt, über die Seite **Script** in Ihre Umgebung hochgeladen und dann auf Jobdefinitionen angewendet.

Zugehörige Tasks

„SQL Server-Anwendungsserver hinzufügen” auf Seite 233
Wenn ein SQL Server-Anwendungsserver hinzugefügt wird, wird ein Bestand der Instanzen und Datenbanken, die dem Anwendungsserver zugeordnet sind, erfasst und zu IBM Spectrum Protect Plus hinzugefügt. Dieser Prozess ermöglicht es Ihnen, Sicherungs- und Zurückschreibungsjobs auszuführen und Berichte zu erstellen.

„SQL Server-Daten sichern” auf Seite 235
Verwenden Sie einen Sicherungsjob, um SQL Server-Umgebungen mit Momentaufnahmen zu sichern.

Oracle-Daten sichern und zurückschreiben

Um Oracle-Inhalt schützen zu können, registrieren Sie zunächst die Oracle-Instanz, damit sie von IBM Spectrum Protect Plus erkannt wird. Erstellen Sie dann Jobs für Sicherungs- und Zurückschreibungsoperationen.

Stellen Sie sicher, dass Ihre Oracle-Umgebung die in „Oracle-Anforderungen” auf Seite 36 beschriebenen Systemanforderungen erfüllt.

Oracle-Anwendungsserver hinzufügen

Wenn ein Oracle-Anwendungsserver hinzugefügt wird, wird ein Bestand der Instanzen und Datenbanken, die dem Anwendungsserver zugeordnet sind, erfasst und zu IBM Spectrum Protect Plus hinzugefügt. Dieser Prozess ermöglicht es Ihnen, Sicherungs- und Zurückschreibungsjobs auszuführen und Berichte zu erstellen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Oracle-Anwendungsserver zu registrieren.

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Oracle** > **Sicherung**.
2. Klicken Sie auf **Anwendungsserver verwalten**.
3. Klicken Sie auf **Anwendungsserver hinzufügen**, um die Hostmaschine hinzuzufügen.
4. Geben Sie im Fenster **Anwendungseigenschaften** die Hostadresse ein.

Die Hostadresse ist eine auflösbare IP-Adresse oder ein auflösbarer Pfad und Maschinenname.

5. Wählen Sie **Benutzer** oder **SSH-Schlüssel** aus.

Option	Bezeichnung
Benutzer	Klicken Sie auf diese Option, um einen vorhandenen Benutzer anzugeben oder eine Benutzer-ID und ein Kennwort einzugeben. Für den Benutzer müssen **sudo**-Berechtigungen definiert sein. Füllen Sie die Felder wie folgt aus: **Vorhandenen Benutzer verwenden** Wählen Sie dieses Kontrollkästchen aus, um einen zuvor eingegebenen Benutzernamen und ein zuvor eingegebenes Kennwort für den Anwendungsserver zu verwenden. Wählen Sie einen Benutzernamen aus der Liste **Benutzer auswählen** aus. **Benutzer-ID** Geben Sie Ihren Benutzernamen für den Anwendungsserver ein. Wenn die virtuelle Maschine einer Domäne zugeordnet ist, folgt die Benutzeridentität dem Standardformat *Domäne**Name*. Ist der Benutzer ein lokaler Administrator, verwenden Sie das Format *lokaler_Administrator*. Nur für die Kerberos-basierte Authentifizierung muss die Benutzeridentität im Format Benutzername@FQDN angegeben werden. Der Benutzername muss sich mit dem registrierten Kennwort authentifizieren können, um ein Ticket-Granting-Ticket (TGT) vom Key-Distribution-Center (KDC) in der Domäne anzufordern, die mit dem vollständig qualifizierten Domänennamen (FQDN) angegeben wird. **Kennwort** Geben Sie Ihr Kennwort für den Anwendungsserver ein.
SSH-Schlüssel	Klicken Sie auf diese Option, um einen SSH-Schlüssel zu verwenden. Wählen Sie einen Schlüssel aus der Liste **SSH-Schlüssel auswählen** aus.

6. Um Multithread-Datenbanken in Oracle 12c und höheren Versionen zu schützen, stellen Sie Berechtigungsnachweise für die Datenbanken bereit:
   a) Klicken Sie auf **Datenbanken abrufen**, um die Oracle-Datenbanken auf dem Host-Server zu erkennen und aufzulisten, der hinzugefügt wird.

      Jede Oracle-Datenbank wird mit dem Namen, dem Status und einer Angabe aufgelistet, ob zuvor Berechtigungsnachweise für die Datenbank angegeben wurden.

   b) Klicken Sie für jede Multithread-Datenbank, die geschützt werden soll, auf **Berechtigungsnachweis definieren** und geben Sie die Benutzer-ID und das Kennwort an. Alternativ können Sie einen vorhandenen Benutzer aus der Liste **Benutzer auswählen** auswählen.

      Sie müssen die Berechtigungsnachweise eines Oracle-Datenbankbenutzers angeben, der über SYSDBA-Berechtigungen verfügt.

7. Definieren Sie in **Maximale Anzahl gleichzeitig verwendeter Datenbanken** die maximale Anzahl der Datenbanken, die gleichzeitig auf dem Server gesichert werden.

   Die Serverleistung wird beeinflusst, wenn viele Datenbanken gleichzeitig gesichert werden, da jede Datenbank mehrere Threads verwendet und Bandbreite verbraucht, wenn Daten kopiert werden. Verwenden Sie diese Option, um die Auswirkungen auf Serverressourcen zu steuern und die Auswirkungen auf den Produktionsbetrieb zu minimieren.

8. Klicken Sie auf **Speichern**. IBM Spectrum Protect Plus bestätigt eine Netzverbindung, fügt den Anwendungsserver zur IBM Spectrum Protect Plus-Datenbank hinzu und katalogisiert dann die Instanz.

   Wird eine Nachricht angezeigt, die angibt, dass die Verbindung nicht erfolgreich ist, überprüfen Sie Ihre Eingaben. Sind Ihre Eingaben korrekt und ist die Verbindung nicht erfolgreich, bitten Sie einen Systemadministrator, die Verbindungen zu überprüfen.

Nächste Schritte

Führen Sie die folgende Aktion aus, nachdem Sie den Oracle-Anwendungsserver hinzugefügt haben:

Aktion	Vorgehensweise
Fügen Sie dem Anwendungsserver Benutzerberechtigungen hinzu.	Siehe „Rolle erstellen” auf Seite 317.

Zugehörige Konzepte

„Benutzerzugriff verwalten” auf Seite 311
Sie können mithilfe der rollenbasierten Zugriffssteuerung die Ressourcen und Berechtigungen festlegen, die IBM Spectrum Protect Plus-Benutzeraccounts zur Verfügung stehen.

Zugehörige Tasks

„Oracle-Daten sichern” auf Seite 247
Verwenden Sie einen Sicherungsjob, um Oracle-Umgebungen mit Momentaufnahmen zu sichern.

„Oracle-Daten zurückschreiben” auf Seite 250
Verwenden Sie einen Zurückschreibungsjob, um eine Oracle-Umgebung aus Momentaufnahmen zurückzuschreiben. IBM Spectrum Protect Plus erstellt einen vSnap-Klon aus der Version, die während der Jobdefinitionserstellung ausgewählt wurde, und erstellt eine Network Files System-Freigabe (NFS-Freigabe). Der IBM Spectrum Protect Plus-Agent stellt dann die Freigabe auf dem Oracle-Server bereit, auf dem der Zurückschreibungsjob ausgeführt werden soll. Für Oracle Real Application Cluster (RAC) wird der Zurückschreibungsjob auf allen Knoten in dem Cluster ausgeführt.

Oracle-Ressourcen erkennen

Oracle-Ressourcen werden automatisch erkannt, nachdem der Anwendungsserver IBM Spectrum Protect Plus hinzugefügt wurde. Sie können jedoch einen Bestandsjob ausführen, um alle Änderungen zu finden, die seit dem Hinzufügen des Anwendungsservers aufgetreten sind.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Bestandsjob auszuführen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Oracle** > **Sicherung**.
2. Wählen Sie in der Liste der Oracle-Instanzen eine Instanz aus oder klicken Sie auf den Link für die Instanz, um zu der gewünschten Ressource zu navigieren. Wenn beispielsweise ein Bestandsjob für eine einzelne Datenbank in der Instanz ausgeführt werden soll, klicken Sie auf den Instanzlink und wählen Sie dann eine virtuelle Maschine aus.
3. Klicken Sie auf **Bestandsverarbeitung ausführen**.

Verbindung zu einem Oracle-Anwendungsserver testen

Sie können die Verbindung zu einem Oracle-Host testen. Die Testfunktion verifiziert die Kommunikation mit dem Host testet DNS-Einstellungen zwischen der virtuellen IBM Spectrum Protect-Appliance und dem Host.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Verbindung zu testen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Oracle** > **Sicherung**.
2. Klicken Sie auf **Anwendungsserver verwalten**.
3. Klicken Sie in der Liste der Hosts im Menü **Aktionen** für den Host auf **Testen**.

Oracle-Daten sichern

Verwenden Sie einen Sicherungsjob, um Oracle-Umgebungen mit Momentaufnahmen zu sichern.

Vorbereitende Schritte

Beachten Sie die folgenden Informationen:

- Um sicherzustellen, dass Dateisystemberechtigungen korrekt beibehalten werden, wenn IBM Spectrum Protect Plus Oracle-Daten zwischen Servern versetzt, stellen Sie sicher, dass die Benutzer- und Grup-

pen-IDs der Oracle-Benutzer (z. B. oracle, oinstall, dba) auf allen Servern konsistent sind. Empfohlene UID- und GID-Werte finden Sie in der Oracle-Dokumentation.

- Wird ein Oracle-Bestandsjob zu derselben Zeit wie ein Oracle-Sicherungsjob oder kurz nach einem Oracle-Sicherungsjob ausgeführt, können aufgrund von temporären Mounts, die während des Sicherungsjobs erstellt werden, Kopierfehler auftreten. Planen Sie als Best Practice Oracle-Bestandsjobs so, dass sie sich nicht mit Oracle-Sicherungsjobs überschneiden.
- Vermeiden Sie das Konfigurieren der Protokollsicherung für eine einzelne Oracle-Datenbank mithilfe mehrerer Sicherungsjobs. Wenn eine einzelne Oracle-Datenbank mehreren Jobdefinitionen mit aktivierter Protokollsicherung hinzugefügt wird, kann eine Protokollsicherung von einem Job ein Protokoll abschneiden, bevor es vom nächsten Job gesichert wird. Dies kann zur Folge haben, dass Jobs für Zurückschreibungen nach Zeitpunkt fehlschlagen.
- Die Wiederherstellung nach Zeitpunkt wird nicht unterstützt, wenn eine oder mehrere Datendateien der Datenbank in dem Zeitraum zwischen dem ausgewählten Zeitpunkt und der Zeit hinzugefügt werden, zu der der vorherige Sicherungsjob ausgeführt wurde.

Führen Sie die folgenden Aktionen aus:

- Bevor ein IBM Spectrum Protect Plus-Benutzer Sicherungs- und Zurückschreibungsoperationen implementieren kann, müssen dem Benutzer Rollen und Ressourcengruppen zugeordnet werden. Erteilen Sie Benutzern mithilfe des Fensters **Accounts** Zugriff auf Ressourcen und Sicherungs- und Zurückschreibungsoperationen. Weitere Informationen finden Sie in Kapitel 13, „Benutzerzugriff verwalten", auf Seite 311.
- Registrieren Sie die Provider, die gesichert werden sollen. Weitere Informationen finden Sie in „Oracle-Anwendungsserver hinzufügen" auf Seite 245.
- Konfigurieren Sie SLA-Richtlinien. Weitere Informationen finden Sie in „Sicherungsrichtlinien erstellen" auf Seite 75.

Informationen zu diesem Vorgang

Während der anfänglichen Basissicherung erstellt IBM Spectrum Protect Plus einen vSnap-Datenträger und eine NFS-Freigabe. Bei Teilsicherungen wird der zuvor erstellte Datenträger wiederverwendet. Der IBM Spectrum Protect Plus-Agent stellt die Freigabe auf dem Oracle-Server bereit, auf dem die Sicherung ausgeführt werden soll.

Im Fall von Oracle Real Application Cluster (RAC) wird die Sicherung auf jedem Knoten im Cluster ausgeführt. Wenn die Sicherung abgeschlossen ist, hebt der IBM Spectrum Protect Plus-Agent die Bereitstellung der Freigabe auf dem Oracle-Server auf und erstellt eine vSnap-Momentaufnahme des Sicherungsdatenträgers.

IBM Spectrum Protect Plus kann Multithread-Datenbanken in Oracle 12c und höheren Versionen schützen. Anweisungen zum Aktivieren von IBM Spectrum Protect Plus zum Schützen von Multithread-Datenbanken finden Sie in „Oracle-Anwendungsserver hinzufügen" auf Seite 245.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Oracle-Sicherungsjob zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Oracle**.
2. Wählen Sie Oracle-Ausgangsverzeichnisse, Datenbanken und ASM-Plattengruppen aus, die gesichert werden sollen. Verwenden Sie die Suchfunktion, um nach verfügbaren Instanzen zu suchen.
3. Klicken Sie auf **SLA-Richtlinie auswählen**, um eine oder mehrere SLA-Richtlinien, die Ihre Sicherungsdatenkriterien erfüllen, zur Jobdefinition hinzuzufügen.
4. Um die Jobdefinition mithilfe von Standardoptionen zu erstellen, klicken Sie auf **Speichern**.

   Der Job wird wie mit den von Ihnen ausgewählten SLA-Richtlinien definiert ausgeführt. Um den Job manuell auszuführen, klicken Sie auf **Jobs und Operationen** > **Zeitplan**. Wählen Sie den Job aus und klicken Sie auf **Aktionen** > **Starten**.

   Tipp: Die Schaltfläche **Ausführen** ist nur für die Sicherung einer einzelnen Datenbank aktiviert; auf die Datenbank muss außerdem eine SLA-Richtlinie angewendet sein.

5. Um Optionen zu editieren, bevor die Jobdefinition erstellt wird, klicken Sie auf **Optionen auswählen**. Definieren Sie die Jobdefinitionsoptionen.

   Protokollsicherung aktivieren

   Protokollsicherung aktivieren muss ausgewählt werden, um die Zurückschreibung nach Zeitpunkt in Oracle zu ermöglichen.

   Wählen Sie **Protokollsicherung aktivieren** aus, um es IBM Spectrum Protect Plus zu ermöglichen, automatisch einen Protokollsicherungsdatenträger zu erstellen und den Datenträger für den Anwendungsserver bereitzustellen. IBM Spectrum Protect Plus erkennt dann automatisch die primäre Position des vorhandenen archivierten Protokolls und verwendet cron, um einen geplanten Job zu konfigurieren. Der geplante Job führt eine Transaktionsprotokollsicherung an der primären Position mit diesem Protokollsicherungsdatenträger in der Häufigkeit aus, die mit der Einstellung für **Häufigkeit** angegeben wird.

   Die **Häufigkeit** kann auf einen Wert gesetzt werden, der von der Häufigkeit der Datenbanksicherung unabhängig ist, die in den Einstellungen für die SLA-Richtlinie angegeben wird. Beispielsweise kann die SLA-Richtlinie so konfiguriert werden, dass die Datenbank einmal pro Tag gesichert wird, während die Häufigkeit der Protokollsicherung auf einmal pro 30 Minuten gesetzt werden könnte.

   Für Oracle RAC stellt IBM Spectrum Protect Plus den Datenträger auf jedem Clusterknoten bereit und konfiguriert den Cron-Job auf jedem Clusterknoten. Wenn der Zeitplan ausgelöst wird, werden die Jobs intern koordiniert, um sicherzustellen, dass jeder aktive Knoten die Protokollsicherung ausführt und die anderen Knoten keine Aktion durchführen.

   IBM Spectrum Protect Plus verwaltet automatisch die Aufbewahrung von Protokollen auf dem eigenen Protokollsicherungsdatenträger auf der Basis der Aufbewahrungseinstellungen in der SLA-Richtlinie.

   Wählen Sie **Quellenprotokolle nach erfolgreicher Sicherung abschneiden** aus, um ältere archivierte Protokolle automatisch an der primären Datenbankposition für archivierte Protokolle zu löschen. Wird die Option abgewählt, werden archivierte Protokolle am primären Protokollziel nicht gelöscht und Datenbankadministratoren müssen weiterhin diese Protokolle mit ihren vorhandenen Protokollaufbewahrungsrichtlinien verwalten. Wird die Option ausgewählt, löscht IBM Spectrum Protect Plus ältere nicht benötigte archivierte Protokolle an der primären Protokollposition am Ende jeder erfolgreichen Datenbanksicherung.

   Wenn die Option **Quellenprotokolle nach erfolgreicher Sicherung abschneiden** ausgewählt wird, definieren Sie die Aufbewahrung von primären Protokollen mit der Einstellung für **Aufbewahrungsdauer des primären Protokolls in Tagen**. Diese Einstellung steuert die Menge der archivierten Protokolle, die an der primären Position für archivierte Protokolle aufbewahrt werden. Wird beispielsweise **Aufbewahrungsdauer des primären Protokolls in Tagen** auf **3** gesetzt, löscht IBM Spectrum Protect Plus am Ende jeder erfolgreichen Datenbanksicherung alle archivierten Protokolle, die älter als drei Tage sind, an der primären Position für archivierte Protokolle.

   Maximale Anzahl paralleler Datenströme pro Datenbank

   Definieren Sie die maximale Anzahl Datenströme pro Datenbank zum Sicherungsspeicher. Diese Einstellung gilt für jede Datenbank in der Jobdefinition. Mehrere Datenbanken können parallel gesichert werden, wenn der Wert der Option auf **1** gesetzt wird. Mehrere parallele Datenströme können die Sicherungsgeschwindigkeit verbessern, die Nutzung hoher Bandbreite kann sich jedoch auf die Systemgesamtleistung auswirken.
6. Wenn die jobspezifischen Informationen korrekt sind, klicken Sie auf **Speichern**.
7. Um zusätzliche Optionen zu konfigurieren, klicken Sie auf das Feld **Richtlinienoptionen**, das dem Job im Abschnitt **SLA-Richtlinienstatus** zugeordnet ist. Definieren Sie die zusätzlichen Richtlinienoptionen:

   Vorscripts und Nachscripts

   Führen Sie ein Vorscript oder Nachscript aus. Vorscripts und Nachscripts sind Scripts, die vor oder nach der Ausführung eines Jobs auf Jobebene ausgeführt werden können. Windows-basierte Maschinen unterstützen Batch- und PowerShell-Scripts, während Linux-basierte Maschinen Shell-Scripts unterstützen.

Wählen Sie im Abschnitt **Vorscript** oder **Nachscript** ein hochgeladenes Script und einen Anwendungs- oder Scriptserver aus, auf dem das Script ausgeführt wird. Um einen Anwendungsserver auszuwählen, auf dem das Script ausgeführt wird, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Scripts und Scriptserver werden auf der Seite **Systemkonfiguration** > **Script** konfiguriert.

Um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt, wählen Sie **Job/Task bei Scriptfehler fortsetzen** aus.

Wenn diese Option aktiviert wird und ein Vorscript oder Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird versucht, die Sicherungs- oder Zurückschreibungsoperation auszuführen, und der Taskstatus für das Vorscript wird als ABGESCHLOSSEN zurückgemeldet. Wenn ein Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird der Taskstatus für das Nachscript als ABGESCHLOSSEN zurückgemeldet.

Wenn diese Option inaktiviert wird, wird nicht versucht, die Sicherung oder Zurückschreibung auszuführen, und der Taskstatus für das Vorscript oder Nachscript wird als FEHLGESCHLAGEN zurückgemeldet.

Ressourcen ausschließen

Schließen Sie bestimmte Ressourcen mit einzelnen oder mehreren Ausschlussmustern aus dem Sicherungsjob aus. Ressourcen können mit einer exakten Übereinstimmung oder mit Sternen als Platzhalterzeichen, die vor dem Muster (*test) oder hinter dem Muster (test*) angegeben werden, ausgeschlossen werden.

Mehrere Sterne als Platzhalterzeichen werden auch in einem einzelnen Muster unterstützt. Die Muster unterstützen alphanumerische Standardzeichen sowie die folgenden Sonderzeichen: - _ und *.

Trennen Sie mehrere Filter durch ein Semikolon voneinander.

Gesamtsicherung der Ressourcen erzwingen

Erzwingen Sie Basissicherungsoperationen für bestimmte virtuelle Maschinen oder Datenbanken in der Sicherungsjobdefinition. Trennen Sie mehrere Ressourcen durch ein Semikolon voneinander.

Nächste Schritte

Führen Sie die folgende Aktion aus, nachdem Sie die Sicherungsjobdefinition erstellt haben:

Aktion	Vorgehensweise
Erstellen Sie eine Oracle-Zurückschreibungsjobdefinition.	Siehe „Oracle-Daten zurückschreiben” auf Seite 250.

Zugehörige Konzepte

„Scripts für Sicherungs- und Zurückschreibungsoperationen konfigurieren” auf Seite 267
Vorscripts und Nachscripts sind Scripts, die ausgeführt werden können, bevor oder nachdem Sicherungs- und Zurückschreibungsjobs auf Jobebene ausgeführt werden. Unterstützt werden Shell-Scripts für Linux-basierte Systeme sowie Batch- und PowerShell-Scripts für Windows-basierte Systeme. Scripts werden lokal erstellt, über die Seite **Script** in Ihre Umgebung hochgeladen und dann auf Jobdefinitionen angewendet.

Oracle-Daten zurückschreiben

Verwenden Sie einen Zurückschreibungsjob, um eine Oracle-Umgebung aus Momentaufnahmen zurückzuschreiben. IBM Spectrum Protect Plus erstellt einen vSnap-Klon aus der Version, die während der Jobdefinitionserstellung ausgewählt wurde, und erstellt eine Network Files System-Freigabe (NFS-Freigabe). Der IBM Spectrum Protect Plus-Agent stellt dann die Freigabe auf dem Oracle-Server bereit, auf dem der Zurückschreibungsjob ausgeführt werden soll. Für Oracle Real Application Cluster (RAC) wird der Zurückschreibungsjob auf allen Knoten in dem Cluster ausgeführt.

Vorbereitende Schritte

Die folgenden Voraussetzungen müssen erfüllt sein:

- Erstellen Sie einen Oracle-Sicherungsjob und führen Sie ihn aus. Anweisungen finden Sie in „Oracle-Daten sichern” auf Seite 247.
- Bevor ein IBM Spectrum Protect Plus-Benutzer Daten zurückschreiben kann, müssen dem Benutzer die entsprechenden Rollen und Ressourcengruppen zugeordnet werden. Erteilen Sie Benutzern mithilfe des Fensters **Accounts** Zugriff auf Ressourcen und Sicherungs- und Zurückschreibungsoperationen. Anweisungen finden Sie in Kapitel 13, „Benutzerzugriff verwalten”, auf Seite 311.

Beachten Sie die folgenden Einschränkungen:

- Die Wiederherstellung nach Zeitpunkt wird nicht unterstützt, wenn eine oder mehrere Datendateien der Datenbank in dem Zeitraum zwischen dem ausgewählten Zeitpunkt und der Zeit hinzugefügt wurden, zu der der vorherige Sicherungsjob ausgeführt wurde.
- Wenn eine Oracle-Datenbank bereitgestellt, aber während eines Sicherungsjobs nicht geöffnet wird, kann IBM Spectrum Protect Plus die Einstellungen bezüglich der automatischen Erweiterbarkeit (**autoextensibility**) und der maximalen Größe für die temporären Datenbankdateien (**tempfiles**) nicht bestimmen. Wenn eine Datenbank von diesem Zurückschreibungspunkt zurückgeschrieben wird, kann IBM Spectrum Protect Plus die temporären Dateien (**tempfiles**) nicht mit den ursprünglichen Einstellungen erneut erstellen, da sie unbekannt sind. Stattdessen werden die temporären Dateien (**tempfiles**) mit den Standardeinstellungen "AUTOEXTEND ON" und "MAXSIZE 32767M" erstellt. Nachdem der Zurückschreibungsjob ausgeführt wurde, können Sie die Einstellungen manuell aktualisieren.
- Bei einer Zurückschreibung aus einem IBM Spectrum Protect-Archiv werden Dateien vom Band in einen Staging-Pool migriert, bevor der Job gestartet wird. Abhängig von der Größe der Zurückschreibung kann dieser Prozess mehrere Stunden dauern.

Informationen zu diesem Vorgang

Die folgenden Zurückschreibungsmodi werden unterstützt:

Instant Access-Modus
Im Instant Access-Modus wird keine weitere Aktion ausgeführt, nachdem die Freigabe bereitgestellt wurde. Benutzer können jede angepasste Wiederherstellung mithilfe der Dateien auf dem vSnap-Datenträger ausführen.

Testmodus
Im Testmodus erstellt der Agent eine neue Datenbank, indem er die Datendateien direkt vom vSnap-Datenträger verwendet.

Produktionsmodus
Im Produktionsmodus schreibt der Agent zunächst die Dateien vom vSnap-Datenträger in den primären Speicher zurück und erstellt dann unter Verwendung der zurückgeschriebenen Dateien die neue Datenbank.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Oracle-Zurückschreibungsjob zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **Anwendungen** > **Oracle** > **Zurückschreibungsjob erstellen**, um den Assistenten "Momentaufnahmezurückschreibung" zu öffnen.

   Tipps:

   - Sie können den Assistenten "Momentaufnahmezurückschreibung" auch öffnen, indem Sie auf **Jobs und Operationen** > **Zurückschreibungsjob erstellen** > **Oracle** klicken.
   - Um eine aktive Zusammenfassung Ihrer Auswahlangaben im Assistenten "Momentaufnahmezurückschreibung" zu erhalten, bewegen Sie den Cursor auf das Informationssymbol im Navigationsfenster des Assistenten.
   - Um die optionalen Seiten im Assistenten zu übergehen, wählen Sie **Optionale Schritte überspringen** aus.
2. Führen Sie auf der Seite **Quellenauswahl** die folgenden Schritte aus:

a) Klicken Sie in der Liste auf eine Quelle, um die Datenbanken anzuzeigen, die für Zurückschreibungsoperationen verfügbar sind. Sie können auch die Suchfunktion verwenden, um nach verfügbaren Instanzen zu suchen, und mithilfe des Filters **Sicht** zwischen den angezeigten Instanzen wechseln.

b) Klicken Sie auf das Plussymbol neben der Datenbank, die als Quelle der Zurückschreibungsoperation verwendet werden soll. Sie können mehrere Datenbanken aus der Liste auswählen.

Die ausgewählten Quellen werden der Zurückschreibungsliste neben der Datenbankliste hinzugefügt. Um einen Eintrag aus der Liste zu entfernen, klicken Sie auf das Minussymbol neben dem Eintrag.

c) Klicken Sie auf **Weiter**, um fortzufahren.

3. Geben Sie auf der Seite **Quellenmomentaufnahme** die Instanz der Datenbank an, die zurückgeschrieben werden soll. Füllen Sie die folgenden Felder aus und klicken Sie auf **Weiter**, um fortzufahren. Einige Felder werden erst angezeigt, nachdem ein zugehöriges Feld ausgewählt wurde.

Option	Beschreibung
Zurückschreibungstyp	Wählen Sie den Typ des Zurückschreibungsjobs aus: **Bedarfsgesteuert: Momentaufnahme** Führt einen einmaligen Zurückschreibungsjob aus einer Datenbankmomentaufnahme aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Bedarfsgesteuert: Zeitpunkt** Führt einen einmaligen Zurückschreibungsjob aus einer Sicherung einer Datenbank nach Zeitpunkt aus. Der Zurückschreibungsjob startet sofort bei Beendigung des Assistenten. **Wiederholt auftretend** Erstellt einen sich wiederholenden Job für die Zurückschreibung nach Zeitpunkt, der gemäß einem Zeitplan ausgeführt wird.
Typ der Zurückschreibungsposition	Wählen Sie einen Typ der Position aus, von der Daten zurückgeschrieben werden sollen: **Site** Die Site, an der Momentaufnahmen gesichert wurden. Die Site wird im Fenster **Systemkonfiguration** > **Site** definiert. **Cloudauslagerung** Der Cloud-Server, auf den Momentaufnahmen ausgelagert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Auslagerung** Der Repository-Server, auf den Momentaufnahmen ausgelagert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert. **Cloudarchivierung** Der Cloud-Server, auf dem Momentaufnahmen archiviert wurden. Der Cloud-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud** definiert. **Repository-Archivierung** Der Repository-Server, auf dem Momentaufnahmen archiviert wurden. Der Repository-Server wird im Fenster **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server** definiert.
Position auswählen	Wenn Sie Daten von einer Site zurückschreiben, wählen Sie eine der folgenden Zurückschreibungspositionen aus:

Option	Beschreibung
	Demo Die Demonstrationssite, von der Momentaufnahmen zurückgeschrieben werden sollen. **Primär** Die primäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. **Sekundär** Die sekundäre Siteposition, von der Momentaufnahmen zurückgeschrieben werden sollen. Wenn Sie Daten von einem Cloud- oder Repository-Server zurückschreiben, wählen Sie einen Server im Menü **Position auswählen** aus.
Datumsauswahl	Geben Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen einen Datumsbereich an, um die verfügbaren Momentaufnahmen innerhalb dieses Datumsbereichs anzuzeigen.
Zurückschreibungspunkt	Wählen Sie für bedarfsgesteuerte Momentaufnahmezurückschreibungsoperationen eine Momentaufnahme aus der Liste der verfügbaren Momentaufnahmen in dem ausgewählten Datenbereich aus.
Alternativen vSnap-Server für den Zurückschreibungsjob verwenden	Wenn Sie Daten aus einer Cloudressource oder von einem Repository-Server zurückschreiben, wählen Sie dieses Kästchen aus, um einen alternativen vSnap-Server anzugeben; wählen Sie dann einen Server im Menü **Alternativen vSnap-Server auswählen** aus. Wenn Sie Daten von einem Zurückschreibungspunkt zurückschreiben, der in eine Cloudressource oder auf einen Repository-Server ausgelagert oder in einer Cloudressource oder auf einem Repository-Server archiviert wurde, wird ein vSnap-Server als Gateway verwendet, um die Operation auszuführen. Standardmäßig stimmt der für die Zurückschreibungsoperation verwendete vSnap-Server mit dem für die Sicherungs- und Auslagerungsoperationen verwendeten vSnap-Server überein. Um die Auslastung auf dem vSnap-Server zu reduzieren, können Sie einen alternativen vSnap-Server als Gateway auswählen.

4. Geben Sie auf der Seite **Ziel definieren** an, wohin die Datenbank zurückgeschrieben werden soll, und klicken Sie auf **Weiter**.

   An ursprüngliche Position zurückschreiben
   Wählen Sie diese Option aus, um die Datenbank auf den ursprünglichen Server zurückzuschreiben.

   An alternative Position zurückschreiben
   Wählen Sie diese Option aus, um die Datenbank an ein lokales Ziel zurückzuschreiben, das nicht mit dem ursprünglichen Server übereinstimmt; wählen Sie dann die alternative Position aus der Liste der verfügbaren Server aus.

5. Definieren Sie auf der Seite **Zurückschreibungsmethode** den Zurückschreibungsjob, der standardmäßig im Test-, Produktions- oder Instant Access-Modus ausgeführt werden soll.

   Für den Test- oder Produktionsmodus können Sie wahlweise einen neuen Namen für die zurückgeschriebene Datenbank eingeben.

   Für den Produktionsmodus können Sie außerdem einen neuen Ordner für die zurückgeschriebene Datenbank angeben, indem Sie die Datenbank erweitern und einen neuen Ordnernamen eingeben.

   Klicken Sie auf **Weiter**, um fortzufahren.

   Nachdem der Job erstellt wurde, kann er im Test-, Produktions- oder Instant Access-Modus im Fenster **Jobsitzungen** ausgeführt werden.

6. Konfigurieren Sie auf der Seite **Joboptionen** weitere Optionen für den Zurückschreibungsjob und klicken Sie auf **Weiter**, um fortzufahren.

Wiederherstellungsoptionen

Definieren Sie die folgenden Optionen für die Wiederherstellung nach Zeitpunkt:

Bis zum Ende der Sicherung wiederherstellen

Mit dieser Option wird die ausgewählte Datenbank mit dem Status zum Zeitpunkt der Erstellung der Sicherung zurückgeschrieben.

Bis zu einem bestimmten Zeitpunkt wiederherstellen

Wenn die Protokollsicherung mithilfe einer Oracle-Sicherungsjobdefinition aktiviert wird, sind Optionen für die Zurückschreibung nach Zeitpunkt verfügbar, wenn eine Oracle-Zurückschreibungsjobdefinition erstellt wird. Wählen Sie eine der folgenden Optionen aus und klicken Sie dann auf **Speichern**:

- **Nach Zeit**. Wählen Sie diese Option aus, um eine Wiederherstellung nach Zeitpunkt anhand eines bestimmten Datums und einer bestimmten Uhrzeit zu konfigurieren.
- **Nach SCN**. Wählen Sie diese Option aus, um eine Wiederherstellung nach Zeitpunkt nach SCN (System Change Number) zu konfigurieren.

IBM Spectrum Protect Plus sucht die Zurückschreibungspunkte unmittelbar vor und nach dem ausgewählten Zeitpunkt. Während der Wiederherstellung werden der ältere Datensicherungsdatenträger und der neuere Protokollsicherungsdatenträger bereitgestellt. Wenn der Zeitpunkt nach der letzten Sicherung liegt, wird ein temporärer Zurückschreibungspunkt erstellt.

Anwendungsoptionen

Definieren Sie die Anwendungsoptionen:

Vorhandene Datenbanken überschreiben

Aktivieren Sie diese Option, um dem Zurückschreibungsjob das Überschreiben der ausgewählten Datenbank zu ermöglichen. Standardmäßig ist diese Option nicht ausgewählt.

Maximale Anzahl paralleler Datenströme pro Datenbank

Definieren Sie die maximale Anzahl Datenströme pro Datenbank aus dem Sicherungsspeicher. Diese Einstellung gilt für jede Datenbank in der Jobdefinition. Mehrere Datenbanken können auch dann parallel zurückgeschrieben werden, wenn der Wert der Option auf 1 gesetzt wird. Mehrere parallele Datenströme können die Zurückschreibungsgeschwindigkeit verbessern, die Nutzung hoher Bandbreite kann sich jedoch auf die Systemgesamtleistung auswirken.

Diese Option ist nur gültig, wenn Sie eine Oracle-Datenbank mit ihrem ursprünglichen Datenbanknamen an die ursprüngliche Position zurückschreiben.

Initialisierungsparameter

Diese Option steuert die Initialisierungsparameter, die verwendet werden, um die wiederhergestellte Datenbank in Oracle-Test- und -Produktionsworkflows zu starten.

Quelle. Diese Option ist die Standardoption. IBM Spectrum Protect Plus verwendet dieselben Initialisierungsparameter wie die Quellendatenbank, aber mit den folgenden Änderungen:

- Parameter, die Pfade enthalten, wie beispielsweise **control_files**, **db_recovery_file_dest** oder **log_archive_dest_***, werden aktualisiert, um die neuen Pfade auf der Basis der umbenannten Mountpunkte der wiederhergestellten Datenträger widerzuspiegeln.
- Parameter wie beispielsweise **audit_file_dest** und **diagnostic_dest** werden aktualisiert, um auf die entsprechende Position unter dem Oracle-Basisverzeichnis auf dem Zielserver zu verweisen, wenn der Pfad von dem des Quellenservers abweicht.
- Wenn ein neuer Name für die Datenbank angegeben wird, werden die Parameter **db_name** und **db_unique_name** aktualisiert, um den neuen Namen widerzuspiegeln.
- Clusterbezogene Parameter, wie beispielsweise **instance_number**, **thread** und **cluster_database**, werden automatisch von IBM Spectrum Protect Plus abhängig von den entsprechenden Werten für das Ziel definiert.

Ziel. Passen Sie die Initialisierungsparameter an, indem Sie eine Schablonendatei mit den Initialisierungsparametern angeben, die von IBM Spectrum Protect Plus verwendet werden.

Der angegebene Pfad muss auf eine einfache Textdatei verweisen, die auf dem Zielserver vorhanden ist und vom IBM Spectrum Protect Plus-Benutzer gelesen werden kann. Die Datei muss im Oracle-`pfile`-Format vorliegen und aus Zeilen im folgenden Format bestehen:

```
Name = Wert
```

Kommentare, die mit dem Zeichen # beginnen, werden ignoriert.

IBM Spectrum Protect Plus liest die Schablonen-`pfile` und kopiert die Einträge in die neue `pfile`, die verwendet wird, um die wiederhergestellte Datenbank zu starten. Die folgenden Parameter in der Schablone werden jedoch ignoriert. Stattdessen definiert IBM Spectrum Protect Plus ihre Werte, um entsprechende Werte aus der Quellendatenbank oder neue Pfade auf der Basis der umbenannten Mountpunkte der wiederhergestellten Datenträger widerzuspiegeln.

- **control_files**
- **db_block_size**
- **db_create_file_dest**
- **db_recovery_file_dest**
- **log_archive_dest**
- **spfile**
- **undo_tablespace**

Außerdem werden clusterbezogene Parameter, wie beispielsweise **instance_number**, **thread** und **cluster_database** automatisch von IBM Spectrum Protect Plus abhängig von den entsprechenden Werten für das Ziel definiert.

Erweiterte Optionen

Definieren Sie die erweiterten Jobdefinitionsoptionen:

Bereinigung direkt beim Fehlschlagen des Jobs ausführen

Aktivieren Sie diese Option, um zugeordnete Ressourcen automatisch im Rahmen einer Zurückschreibungsoperation zu bereinigen, wenn die Wiederherstellung fehlschlägt.

Sitzungsüberschreibung zulassen

Wählen Sie diese Option aus, um eine vorhandene Datenbank während der Wiederherstellung durch eine Datenbank mit demselben Namen zu ersetzen. Wenn eine Instant Disk Restore-Operation für eine Datenbank ausgeführt wird und eine andere Datenbank mit demselben Namen bereits auf dem Zielhost oder -cluster ausgeführt wird, fährt IBM Spectrum Protect Plus die vorhandene Datenbank herunter, bevor die wiederhergestellte Datenbank gestartet wird. Wenn diese Option nicht ausgewählt wird, schlägt der Zurückschreibungsjob fehl, wenn IBM Spectrum Protect Plus eine vorhandene aktive Datenbank mit demselben Namen findet.

Mit Zurückschreibungen der anderen ausgewählten Datenbanken fortfahren, auch wenn eine Zurückschreibung fehlschlägt

Aktivieren Sie diese Option, um mit der Wiederherstellung einer Ressource in einer Serie fortzufahren, wenn die Wiederherstellung der vorherigen Ressource fehlschlägt. Wenn diese Option nicht aktiviert wird, wird der Zurückschreibungsjob gestoppt, wenn die Wiederherstellung einer Ressource fehlschlägt.

Protokollpriorität (nur Instant Access)

Sind mehrere Speicherprotokolle verfügbar, wählen Sie das Protokoll aus, das in dem Job Priorität haben soll. Die verfügbaren Protokolle sind **iSCSI** und **Fibre Channel**.

Mountpunktpräfix

Geben Sie für Instant Access-Zurückschreibungsoperationen das Präfix für den Pfad an, für den der Mountpunkt bereitgestellt werden soll.

7. Optional: Geben Sie auf der Seite **Scripts anwenden** Scripts an, die vor oder nach der Ausführung einer Operation auf Jobebene ausgeführt werden können. Batch- und PowerShell-Scripts werden unter Windows-Betriebssystemen unterstützt; Shell-Scripts werden unter Linux-Betriebssystemen unterstützt.

Vorscript
Wählen Sie dieses Kontrollkästchen aus, um ein hochgeladenes Script und einen Anwendungs- oder Scriptserver auszuwählen, auf dem das Vorscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, auf dem das Vorscript ausgeführt wird, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Scripts und Scriptserver werden auf der Seite **Systemkonfiguration** > **Script** konfiguriert.

Nachscript
Wählen Sie dieses Kontrollkästchen aus, um ein hochgeladenes Script und einen Anwendungs- oder Scriptserver auszuwählen, auf dem das Nachscript ausgeführt wird. Um einen Anwendungsserver auszuwählen, auf dem das Nachscript ausgeführt wird, wählen Sie das Kontrollkästchen **Scriptserver verwenden** ab. Scripts und Scriptserver werden auf der Seite **Systemkonfiguration** > **Script** konfiguriert.

Job/Task bei Scriptfehler fortsetzen
Wählen Sie dieses Kontrollkästchen aus, um die Ausführung des Jobs fortzusetzen, wenn das dem Job zugeordnete Script fehlschlägt.

Wenn Sie dieses Kontrollkästchen auswählen und ein Vorscript oder Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird versucht, die Sicherungs- oder Zurückschreibungsoperation auszuführen, und der Taskstatus für das Vorscript wird als ABGESCHLOSSEN zurückgemeldet. Wenn ein Nachscript die Verarbeitung mit einem Rückkehrcode ungleich null beendet, wird der Taskstatus für das Nachscript als ABGESCHLOSSEN zurückgemeldet.

Wenn Sie dieses Kontrollkästchen abwählen, wird nicht versucht, die Sicherung oder Zurückschreibung auszuführen, und der Taskstatus für das Vorscript oder Nachscript wird als FEHLGESCHLAGEN zurückgemeldet.

8. Führen Sie auf der Seite **Zeitplan** eine der folgenden Aktionen aus:
   - Wenn Sie einen bedarfsgesteuerten Job ausführen, klicken Sie auf **Weiter**.
   - Wenn Sie einen sich wiederholenden Job definieren, geben Sie einen Namen für den Jobzeitplan ein und geben Sie die Häufigkeit und den Startzeitpunkt des Zurückschreibungsjobs an. Klicken Sie auf **Weiter**.
9. Überprüfen Sie auf der Seite **Überprüfen** die Einstellungen Ihres Zurückschreibungsjobs und klicken Sie auf **Übergeben**, um den Job zu erstellen.

Ergebnisse

Ein bedarfsgesteuerter Job startet, nachdem Sie auf **Übergeben** geklickt haben, und der Satz **Bedarfsgesteuerte Zurückschreibung** wird dem Fenster **Jobsitzungen** kurz danach hinzugefügt. Um den Fortschritt der Zurückschreibungsoperation anzuzeigen, erweitern Sie den Job. Sie können die Protokolldatei auch herunterladen, indem Sie auf das Symbol für Herunterladen klicken.

Ein sich wiederholender Job startet zum geplanten Startzeitpunkt, wenn Sie den Zeitplan auf der Seite **Jobs und Operationen** > **Zeitplan** starten.

Alle aktiven Jobs sind auf der Seite **Jobs und Operationen** > **Aktive Jobs** anzeigbar.

Nächste Schritte

Oracle-Datenbanken werden immer im Nicht-Multithread-Modus zurückgeschrieben. Waren die Datenbanken, die zurückgeschrieben wurden, ursprünglich im Multithread-Modus, müssen Sie nach der Ausführung der Zurückschreibungsoperation manuell Berechtigungsnachweise konfigurieren und die Datenbanken in den Multithread-Modus versetzen.

Zugehörige Konzepte

„Scripts für Sicherungs- und Zurückschreibungsoperationen konfigurieren” auf Seite 267
Vorscripts und Nachscripts sind Scripts, die ausgeführt werden können, bevor oder nachdem Sicherungs- und Zurückschreibungsjobs auf Jobebene ausgeführt werden. Unterstützt werden Shell-Scripts für Linux-basierte Systeme sowie Batch- und PowerShell-Scripts für Windows-basierte Systeme. Scripts werden lo-

kal erstellt, über die Seite **Script** in Ihre Umgebung hochgeladen und dann auf Jobdefinitionen angewendet.

Zugehörige Tasks

„Oracle-Anwendungsserver hinzufügen” auf Seite 245
Wenn ein Oracle-Anwendungsserver hinzugefügt wird, wird ein Bestand der Instanzen und Datenbanken, die dem Anwendungsserver zugeordnet sind, erfasst und zu IBM Spectrum Protect Plus hinzugefügt. Dieser Prozess ermöglicht es Ihnen, Sicherungs- und Zurückschreibungsjobs auszuführen und Berichte zu erstellen.

Kapitel 9. IBM Spectrum Protect Plus schützen

Zum Schutz der IBM Spectrum Protect Plus-Anwendung sichern Sie die zugrunde liegenden Datenbanken für Wiederherstellungsszenarios. Konfigurationseinstellungen, registrierte Ressourcen, Zurückschreibungspunkte, Sicherungsspeichereinstellungen, Suchdaten sowie Jobinformationen werden auf einem vSnap-Server gesichert, der in der zugeordneten SLA-Richtlinie definiert ist.

IBM Spectrum Protect Plus-Anwendung sichern

Sichern Sie IBM Spectrum Protect Plus-Konfigurationseinstellungen, SLA-Richtlinien, registrierte Ressourcen, Sicherungsspeichereinstellungen, Zurückschreibungspunkte, Suchdaten sowie importierte Schlüssel und Zertifikate auf einem vSnap-Server, der in der zugeordneten SLA-Richtlinie definiert ist.

Vorbereitende Schritte

Stellen Sie sicher, dass die entsprechende SLA-Richtlinie verfügbar ist. Um Sicherungsjobs zu optimieren, erstellen Sie SLA-Richtlinien speziell für die Sicherung von IBM Spectrum Protect Plus. Um die Systembelastung zu reduzieren, stellen Sie sicher, dass die Ausführung anderer Jobs während des IBM Spectrum Protect Plus-Sicherungsjobs nicht geplant ist. Um eine SLA-Richtlinie zu erstellen, lesen Sie die Informationen in „SLA-Richtlinie erstellen” auf Seite 93.

Einschränkung: Sie können den integrierten vSnap-Server nicht als Ziel der IBM Spectrum Protect Plus-SLA-Sicherungsrichtlinie auswählen. Der integrierte vSnap-Server hat den Namen 'localhost' und wird automatisch installiert, wenn die IBM Spectrum Protect Plus-Appliance anfänglich implementiert wird. Wählen Sie einen sekundären externen vSnap-Server als Ziel aus, wenn eine SLA-Richtlinie für die Sicherung erstellt wird.

Ein IBM Spectrum Protect Plus-Katalog kann in Wiederherstellungsszenarios an dieselbe Position oder an eine alternative IBM Spectrum Protect Plus-Position zurückgeschrieben werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um IBM Spectrum Protect Plus-Daten zu sichern:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **IBM Spectrum Protect Plus** > **Sicherung**.
2. Wählen Sie eine SLA-Richtlinie aus, die der IBM Spectrum Protect Plus-Katalogsicherungsoperation zugeordnet werden soll. Die SLA-Richtlinie definiert die zeitliche Planung der Katalogsicherung zusammen mit den Sicherungsziel-, Replikations- und Auslagerungseinstellungen. Katalogsicherungsdaten können auch in Cloudressourcen und auf Repository-Server ausgelagert werden.
3. Klicken Sie auf **Speichern**, um die Jobdefinition zu erstellen.

Ergebnisse

Der Job wird wie mit den von Ihnen ausgewählten SLA-Richtlinien definiert ausgeführt; Sie können den Job auch manuell ausführen, indem Sie auf **Jobs und Operationen** > **Zeitplan** klicken. Wählen Sie dann den Job auf der Registerkarte **Zeitplan** aus und klicken Sie auf **Aktionen** > **Starten**. Anweisungen finden Sie in „Sicherungsjob starten” auf Seite 83.

IBM Spectrum Protect Plus-Anwendung zurückschreiben

Schreiben Sie IBM Spectrum Protect Plus-Konfigurationseinstellungen, Zurückschreibungspunkte, Suchdaten und Jobinformationen zurück, die auf dem vSnap-Server gesichert wurden. Die Daten können an dieselbe Position oder an eine andere IBM Spectrum Protect Plus-Position zurückgeschrieben werden.

© Copyright IBM Corp. 2017, 2019

Informationen zu diesem Vorgang

Achtung: Eine IBM Spectrum Protect Plus-Zurückschreibungsoperation überschreibt alle Daten an der Position der virtuellen IBM Spectrum Protect Plus-Appliance oder an der Position der alternativen virtuellen Appliance. Alle IBM Spectrum Protect Plus-Operationen werden gestoppt, während die Daten zurückgeschrieben werden. Auf die Benutzerschnittstelle kann nicht zugegriffen werden, und alle aktiven Jobs werden abgebrochen. Alle Momentaufnahmen, die zwischen den Sicherungs- und Zurückschreibungsoperationen erstellt werden, werden nicht gespeichert.

Wird eine ausgelagerte Cloudsicherung zurückgeschrieben, muss die Cloudressource oder der Repository-Server für die alternative IBM Spectrum Protect Plus-Position registriert werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um IBM Spectrum Protect Plus-Daten zurückzuschreiben:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **IBM Spectrum Protect Plus** > **Zurückschreibung**.
2. Wählen Sie einen vSnap-Server, eine Cloudressource oder einen Repository-Server aus.

   Daten können in Wiederherstellungsszenarios an dieselbe Position oder an eine alternative Position zurückgeschrieben werden.

   Verfügbare Momentaufnahmen für den Server werden angezeigt.
3. Klicken Sie für die Katalogmomentaufnahme, die zurückgeschrieben werden soll, auf **Zurückschreiben**.
4. Wählen Sie einen der folgenden Zurückschreibungsmodi aus:

   Katalog zurückschreiben und alle geplanten Jobs aussetzen
   Der Katalog wird zurückgeschrieben und alle geplanten Jobs verbleiben in einem Aussetzstatus. Es werden keine geplanten Jobs gestartet, wodurch die Validierung und der Test von Katalogeinträgen und die Erstellung neuer Jobs ermöglicht wird. Normalerweise wird diese Option in DevOps-Anwendungsfällen verwendet.

   Katalog zurückschreiben
   Der Katalog wird zurückgeschrieben und alle geplanten Jobs werden weiterhin wie in der Katalogsicherung erfasst ausgeführt. Normalerweise wird diese Option bei der Wiederherstellung nach einem Katastrophenfall verwendet.
5. Klicken Sie auf **Zurückschreiben**.
6. Um den Zurückschreibungsjob auszuführen, klicken Sie im Dialogfenster auf **Ja**.

IBM Spectrum Protect Plus-Zurückschreibungspunkte verwalten

Sie können das Fenster **Zurückschreibungspunktaufbewahrung** verwenden, um im IBM Spectrum Protect Plus-Katalog nach Zurückschreibungspunkten nach Sicherungsjobnamen zu suchen, ihre Erstellungs- und Verfallsdaten anzuzeigen und die zugeordnete Aufbewahrung zu überschreiben.

Informationen zu diesem Vorgang
Wenn eine Jobsitzung als verfallen definiert wird, werden eine Momentaufnahme und der zugehörige Wiederherstellungspunkt nicht entfernt, wenn die Momentaufnahme durch eine Replikations- oder Auslagerungsbeziehung gesperrt wird. Führen Sie den für die Replikation oder Auslagerung aktivierten Job aus, um die Sperre einer späteren Momentaufnahme zuzuordnen. Die Momentaufnahme und der Wiederherstellungspunkt werden bei der nächsten Ausführung des Verwaltungsjobs entfernt.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Jobsitzung als verfallen zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **IBM Spectrum Protect Plus** > **Zurückschreibungspunktaufbewahrung**.

2. Suchen Sie auf der Registerkarte 'Sicherungssitzungen' nach der gewünschten Jobsitzung oder dem gewünschten Zurückschreibungspunkt. Weitere Informationen zur Verwendung der Suchfunktion finden Sie in Anhang A, „Suchrichtlinien”, auf Seite 331.
3. Verwenden Sie Filter, um das Durchsuchen der Jobtypen und des Datumsbereichs, in dem der zugeordnete Sicherungsjob gestartet wurde, zu optimieren.
4. Klicken Sie auf das Suchsymbol .
5. Wählen Sie die Jobsitzungen aus, die als verfallen definiert werden sollen.
6. Wählen Sie aus der Liste **Aktionen** eine der folgenden Optionen aus:
   - **Als verfallen definieren** wird verwendet, um eine einzelne Jobsitzung als verfallen zu definieren.
   - **Alle Jobsitzungen als verfallen definieren** wird verwendet, um alle nicht verfallenen Jobsitzungen für den ausgewählten Job als verfallen zu definieren.
7. Um den Verfall zu bestätigen, klicken Sie im Dialogfenster auf **Ja**.

Ergebnisse
Die Jobsitzung wird bei der nächsten Ausführung des Verwaltungsjobs entfernt.
Zugehörige Konzepte
„Jobtypen” auf Seite 263
Jobs werden zur Ausführung von Sicherungs-, Zurückschreibungs-, Verwaltungs- und Bestandsoperationen in IBM Spectrum Protect Plus verwendet.

IBM Spectrum Protect Plus-Ressourcen aus dem Katalog löschen

Sie können die Registerkarte **Virtuelle Maschinen/Datenbanken** im Fenster **Zurückschreibungspunktaufbewahrung** verwenden, um Katalogmetadaten als verfallen zu definieren, die einer Ressource im IBM Spectrum Protect Plus-Katalog zugeordnet sind. Ressourcen werden dem Katalog mithilfe von Bestandsjobs hinzugefügt. Wird eine Ressource als verfallen definiert, werden die Metadaten entfernt, die einem Zurückschreibungspunkt im Katalog zugeordnet sind. Dadurch wird Speicherbereich im Katalog freigegeben und der Zurückschreibungspunkt aus Wiederherstellungsanzeigen entfernt.

Informationen zu diesem Vorgang
Wenn eine Ressource im Katalog als verfallen definiert wird, werden die zugeordneten Momentaufnahmen auf einem vSnap-Server oder im sekundären Sicherungsspeicher nicht entfernt.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ressource im Katalog als verfallen zu definieren:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten** > **IBM Spectrum Protect Plus** > **Zurückschreibungspunktaufbewahrung**.
2. Klicken Sie auf die Registerkarte **Virtuelle Maschinen/Datenbanken**.
3. Verwenden Sie den Filter, um nach Ressourcentyp zu suchen, und geben Sie dann einen Suchbegriff ein, um nach einer Ressource nach Namen zu suchen. Weitere Informationen zur Verwendung der Suchfunktion finden Sie in Anhang A, „Suchrichtlinien”, auf Seite 331.
4. Klicken Sie auf das Suchsymbol .
5. Klicken Sie auf das Symbol für Löschen , das einer Ressource zugeordnet ist.
6. Um den Verfall zu bestätigen, klicken Sie im Dialogfenster auf **Ja**.

Ergebnisse
Die Katalogmetadaten, die der Ressource zugeordnet sind, werden aus dem Katalog entfernt.
Zugehörige Konzepte
„Jobtypen” auf Seite 263

Jobs werden zur Ausführung von Sicherungs-, Zurückschreibungs-, Verwaltungs- und Bestandsoperationen in IBM Spectrum Protect Plus verwendet.

Kapitel 10. Jobs und Operationen

Verwenden Sie das Fenster **Jobs und Operationen**, um Jobs zu überwachen, das Jobprotokoll zu überprüfen, Jobs zu planen, aktive Ressourcen anzuzeigen und Jobs und Zeitpläne erneut auszuführen oder anzuhalten.

Um Jobs und Ressourcen anzuzeigen und zu verwalten, klicken Sie auf **Jobs und Operationen** und klicken Sie dann auf die entsprechende Registerkarte:

- **Aktive Jobs**: Zeigt die Sicherungs-, Bestands-, Verwaltungs- und Zurückschreibungsjobs an, die aktiv sind.
- **Jobprotokoll**: Zeigt die Jobs an, die fehlgeschlagen sind, Jobs, deren Verarbeitung mit Warnungen beendet wurde, sowie Jobs, die erfolgreich ausgeführt wurden. Sie können ein Jobprotokoll von der Seite herunterladen, indem Sie den Job auswählen und auf **ZIP-Datei herunterladen** klicken.
- **Aktive Ressourcen**: Zeigt aktive Anwendungs- und Hypervisorressourcen an.
- **Zeitplan**: Zeigt die Jobzeitpläne an. Sie können einen bedarfsgesteuerten Job starten oder einen Zeitplan für einen ausgewählten Job anhalten. Mithilfe des Symbols für Editieren  können Sie einen Jobzeitplan auch editieren.

Es ist auch möglich, bedarfsgesteuerte oder sich wiederholende Zurückschreibungsjobs zu erstellen, indem Sie auf **Zurückschreibungsjob erstellen** klicken. Um Anweisungen zum Erstellen von Zurückschreibungsjobs aufzurufen, klicken Sie auf die Links in der folgenden Tabelle:

Tabelle 22. Zurückschreibungsjobs erstellen

Task	Anweisungen
Zurückschreibungsjobs für Hypervisoren erstellen	Siehe die folgenden Abschnitte: • „VMware-Daten zurückschreiben” auf Seite 116 • „Hyper-V-Daten zurückschreiben” auf Seite 133
Zurückschreibungsjobs für Anwendungen erstellen	Siehe die folgenden Abschnitte: • „Db2-Daten zurückschreiben” auf Seite 157 • „Microsoft Exchange-Datenbanken zurückschreiben” auf Seite 174 • „MongoDB-Daten zurückschreiben” auf Seite 217 • „Oracle-Daten zurückschreiben” auf Seite 250 • „SQL Server-Daten zurückschreiben” auf Seite 239

Jobtypen

Jobs werden zur Ausführung von Sicherungs-, Zurückschreibungs-, Verwaltungs- und Bestandsoperationen in IBM Spectrum Protect Plus verwendet.

Sicherungs- und Zurückschreibungsjobs sind benutzerdefiniert. Nach der Erstellung dieser Jobs können Sie sie jederzeit ändern. Verwaltungs- und Bestandsjobs sind vordefiniert und können nicht geändert werden.

© Copyright IBM Corp. 2017, 2019

Sie können alle Jobs nach Bedarf ausführen, auch wenn ihre Ausführung in einem Zeitplan festgelegt ist. Sie können auch Jobs anhalten und freigeben, deren Ausführung in einem Zeitplan festgelegt ist.

Folgende Jobtypen sind verfügbar:

Sicherung
Ein Sicherungsjob definiert die Ressourcen, die gesichert werden sollen, und die SLA-Richtlinie(n), die auf diese Ressourcen angewendet werden soll(en). Jede SLA-Richtlinie legt den Auführungszeitpunkt des Jobs fest. Sie können den Job mit dem in der SLA-Richtlinie definierten Zeitplan oder nach Bedarf ausführen.

Der Jobname wird automatisch generiert und setzt sich aus dem Ressourcentyp und der für den Job verwendeten SLA-Richtlinie zusammen. Beispielsweise lautet der Name eines Sicherungsjobs für SQL Server-Ressourcen, die der SLA-Richtlinie "Gold" zugeordnet sind, `sql_Gold`.

Zurückschreibung
Ein Zurückschreibungsjob definiert den Zurückschreibungspunkt, von dem Daten zurückgeschrieben werden sollen. Wenn Sie z. B. Hypervisordaten zurückschreiben, könnte der Zurückschreibungspunkt eine virtuelle Maschine sein. Wenn Sie Anwendungsdaten zurückschreiben, könnte der Zurückschreibungspunkt eine Datenbank sein. Sie können einen Zeitplan erstellen, um den Job auszuführen, oder Sie können den Job nach Bedarf ausführen.

Der Jobname ist davon abhängig, ob Sie den Job nach Bedarf oder nach Zeitplan ausführen. Wenn Sie eine Zurückschreibungsoperation nach Bedarf ausführen, wird der Jobname `onDemandRestore` automatisch generiert.

Wenn Sie einen Job für eine Ausführung nach Zeitplan erstellen, müssen Sie einen Jobnamen angeben.

Verwaltung
Der Verwaltungsjob wird einmal täglich ausgeführt, um Ressourcen und zugehörige Objekte zu entfernen, die von IBM Spectrum Protect Plus erstellt werden, wenn ein Job, der sich im Wartestatus befindet, gelöscht wird.

Durch die Bereinigungsprozedur wird Speicherbereich auf Speichereinheiten konsolidiert, der IBM Spectrum Protect Plus-Katalog bereinigt und zugehörige Momentaufnahmen werden entfernt. Darüber hinaus entfernt der Verwaltungsjob katalogisierte Daten, die gelöschten Jobs zugeordnet sind.

Der Jobname lautet `Maintenance`.

Bestand
Ein Bestandsjob wird automatisch ausgeführt, wenn Sie IBM Spectrum Protect Plus eine Ressource hinzufügen. Sie können einen Bestandsjob jedoch jederzeit ausführen, um alle Änderungen festzustellen, die seit dem Hinzufügen der Ressource aufgetreten sind.

Die Bestandsjobnamen lauten `Default Application Server Inventory`, `Default Hypervisor Inventory` und `Default Storage Server Inventory`.

Jobs starten

Sie können einen Job selbst dann bedarfsgesteuert ausführen, wenn die Ausführung des Jobs gemäß einem Zeitplan festgelegt ist.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Job zu starten:

1. Klicken Sie im Navigationsfenster auf **Jobs und Operationen** und klicken Sie auf die Registerkarte **Zeitplan**.
2. Wählen Sie den Job aus, der ausgeführt werden soll, und klicken Sie auf **Aktionen** > **Starten**.
   Der Job wird gestartet und der Registerkarte **Aktive Jobs** hinzugefügt.

Nächste Schritte

Um das Jobprotokoll detailliert anzuzeigen, klicken Sie auf der Registerkarte **Aktive Jobs** auf den Job.

In der Protokollanzeige werden die folgenden Details angezeigt:

- Status: Zeigt an, ob es sich bei der Nachricht um eine Fehler-, Warn- oder Informationsnachricht handelt.
- Zeit: Zeigt die Zeitmarke der Nachricht an.
- ID: Zeigt die eindeutige ID für die Nachricht an, sofern zutreffend.
- Beschreibung: Zeigt den Text der Nachricht an.

Sie können ein Jobprotokoll von der Seite herunterladen, indem Sie auf **ZIP-Datei herunterladen** klicken. Um den Job abzubrechen, klicken Sie auf **Aktionen** > **Abbrechen**.

Jobs anhalten und wiederaufnehmen

Sie können einen geplanten Job oder einen aktiven Job anhalten und wiederaufnehmen. Wenn Sie einen geplanten Job anhalten, wird der Job bis zu seiner Wiederaufnahme nicht ausgeführt.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Jobzeitpläne anzuhalten und freizugeben:

1. Klicken Sie im Navigationsfenster auf **Jobs und Operationen** und klicken Sie auf die Registerkarte **Zeitplan**.
2. Wählen Sie den Job aus, der angehalten werden soll, und klicken Sie auf **Aktionen** > **Zeitplan anhalten**.
3. Um den Jobzeitplan wiederaufzunehmen, klicken Sie auf **Aktionen** > **Zeitplan freigeben**.

Jobs abbrechen

Sie können einen aktiven Job abbrechen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Job abzubrechen:

1. Klicken Sie im Navigationsfenster auf **Jobs und Operationen** und klicken Sie dann auf die Registerkarte **Zeitplan**.
2. Um eine aktive Jobsitzung abzubrechen, klicken Sie auf das Menü **Aktionen**, das dem Job zugeordnet ist, und klicken Sie dann auf **Abbrechen**.

Teilweise ausgeführte Sicherungsjobs erneut ausführen

Wenn die letzte Instanz eines Sicherungsjobs teilweise ausgeführt wurde, können Sie den Job erneut ausführen, um virtuelle Maschinen und Datenbanken, die übersprungen wurden, zu sichern.

Informationen zu diesem Vorgang

Ein Sicherungsjob kann nur mit derselben Sitzungs-ID wie der des ursprünglichen teilweise ausgeführten Sicherungsjobs erneut ausgeführt werden. Im Anschluss an den teilweise ausgeführten Sicherungsjob, den Sie für die erneute Ausführung ausgewählt haben, kann keine erfolgreiche Sicherung derselben Ressource ausgeführt worden sein.

Anmerkung: Sicherungsjobs können nur als Antwort auf einen Hypervisor- oder Datenbanksicherungsfehler erneut ausgeführt werden. Die folgenden Ereignisse erfüllen nicht die Kriterien für Operationen zur erneuten Ausführung von Sicherungsjobs:

- Eine VM-Sicherung wurde mit einem FLI-Fehler beendet.
- Es ist ein Momentaufnahmekomprimierungsfehler für ein Speichersystem aufgetreten.

- Ein Sicherungsjob ist mit einem unbekannten Problem, wie beispielsweise einem Katalogisierungsfehler, fehlgeschlagen.
- In vCenter fehlt eine Ressource.

Für Anwendungen, für die Protokollsicherungen unterstützt werden, werden Protokollsicherungen nicht inaktiviert, wenn die Funktion für die erneute Ausführung verwendet wird. Protokollsicherungen werden für die betreffenden Datenbanken inaktiviert, wenn der Job das nächste Mal ohne die Verwendung der Funktion für die bedarfsgesteuerte Sicherung oder die erneute Ausführung gestartet wird.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine teilweise ausgeführte Sicherungsoperation erneut auszuführen:

1. Klicken Sie im Navigationsfenster auf **Jobs und Operationen** und klicken Sie dann auf die Registerkarte **Jobprotokoll**.
2. Verwenden Sie die Suchfunktion und Filter, um nach der letzten Instanz des Sicherungsjobs zu suchen, der teilweise ausgeführt wurde.
3. Wählen Sie die Jobinstanz aus und klicken Sie dann auf **Erneut ausführen**.

   Anmerkung:

   Wenn der Sicherungsjob nicht erneut ausgeführt werden kann, ist die Option **Erneut ausführen** nicht verfügbar.

   Alle SLA-Optionen und alle Ausschlüsse, die dem ursprünglichen Job zugeordnet sind, werden in die Operation zur erneuten Ausführung eingeschlossen. Änderungen an Optionen oder Ausschlüssen, die nach der Ausführung der Teilsicherung durchgeführt wurden, werden nicht angewendet. Wenn der Job zur erneuten Ausführung erfolgreich ausgeführt wird, wird die Jobzusammenfassung aktualisiert, um die erfolgreiche Ausführung anzuzeigen.

Einzelne Ressource sichern

Wenn ein Hypervisor oder Anwendungsserver einer SLA-Richtlinie zugeordnet ist, kann eine einzelne virtuelle Maschine oder Anwendung sofort gesichert werden, indem eine bedarfsgesteuerte Sicherungsoperation ausgeführt wird. Wählen Sie **Ausführen** in einer Sicherungsanzeige für den Hypervisor oder Anwendungsserver aus, um eine bedarfsgesteuerte Sicherungsoperation auszuführen. Diese Option ist aktiviert, wenn eine vorhandene SLA-Richtlinie der Ressource zugeordnet ist.

Informationen zu diesem Vorgang
Die erneute Ausführung eines Sicherungsjobs für eine einzelne Ressource ist nur für Sicherungsoperationen, aber nicht für Replikations- oder Auslagerungsoperationen gültig.

Für Anwendungen, für die Protokollsicherungen unterstützt werden, werden Protokollsicherungen nicht inaktiviert, wenn die Funktion für die bedarfsgesteuerte Sicherung oder die erneute Ausführung verwendet wird. Protokollsicherungen werden für die betreffenden Datenbanken inaktiviert, wenn der Job das nächste Mal ohne die Verwendung der Funktion für die bedarfsgesteuerte Sicherung oder die erneute Ausführung gestartet wird.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um den bedarfsgesteuerten Sicherungsjob für eine einzelne virtuelle Maschine oder einen einzelnen Anwendungsserver auszuführen:

1. Klicken Sie im Navigationsfenster auf **Schutz verwalten**. Wählen Sie abhängig vom Typ der Sicherungsoperation **Hypervisoren** > **Sicherung** oder **Anwendungen** > **Sicherung** aus.
2. Klicken Sie auf die aufgelisteten Instanzen, um die zugeordneten Ressourcen der virtuellen Maschine oder die zugeordneten Anwendungsressourcen anzuzeigen.

   Der Hypervisor oder Anwendungsserver muss einer vorhandenen SLA-Richtlinie zugeordnet sein.

3. Klicken Sie auf **Ausführen**.

   Wenn die virtuelle Maschine oder Anwendung zu mehreren SLA-Richtlinien gehört, wählen Sie die SLA-Richtlinie aus, die für den bedarfsgesteuerten Job ausgeführt werden soll.
4. Klicken Sie zur Bestätigung des Sicherungsjob im Dialogfenster auf **OK**.

Scripts für Sicherungs- und Zurückschreibungsoperationen konfigurieren

Vorscripts und Nachscripts sind Scripts, die ausgeführt werden können, bevor oder nachdem Sicherungs- und Zurückschreibungsjobs auf Jobebene ausgeführt werden. Unterstützt werden Shell-Scripts für Linux-basierte Systeme sowie Batch- und PowerShell-Scripts für Windows-basierte Systeme. Scripts werden lokal erstellt, über die Seite **Script** in Ihre Umgebung hochgeladen und dann auf Jobdefinitionen angewendet.

Vorbereitende Schritte

Beachten Sie die folgenden Hinweise zur Verwendung von Scripts mit Hypervisoren:

- Für den Benutzer, der das Script ausführt, muss die zur Ausführung von Vorscripts und Nachscripts erforderliche Berechtigung **Als Service anmelden** aktiviert sein. Weitere Informationen zu dieser Berechtigung finden Sie in Add the Log on as a service Right to an Account.
- Windows Remote Shell (WinRM) muss aktivert sein.

Script hochladen

Unterstützte Scripts umfassen Shell-Scripts für Linux-basierte Maschinen sowie Batch- und PowerShell-Scripts für Windows-basierte Maschinen. Scripts müssen unter Verwendung des zugeordneten Dateiformats für das Betriebssystem erstellt werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Script hochzuladen:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Script**.
2. Klicken Sie im Abschnitt **Scripts** auf **Script hochladen**.

   Das Fenster **Script hochladen** wird angezeigt.
3. Klicken Sie auf **Durchsuchen**, um ein lokales Script, das hochgeladen werden soll, auszuwählen.
4. Klicken Sie auf **Speichern**.

   Das Script wird in der Tabelle **Scripts** angezeigt und kann auf unterstützte Jobs angewendet werden.

Nächste Schritte

Führen Sie die folgende Aktion aus, nachdem Sie das Script hochgeladen haben:

Aktion	Vorgehensweise
Fügen Sie das Script einem Server hinzu, auf dem es ausgeführt wird.	Siehe „Script einem Server hinzufügen” auf Seite 267.

Script einem Server hinzufügen

Fügen Sie das Script einem Server hinzu, auf dem es ausgeführt wird.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Script für einen Server anzugeben:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Script**.
2. Klicken Sie im Abschnitt **Scriptserver** auf **Scriptserver hinzufügen**.

   Das Fenster **Eigenschaften für Scriptserver** wird angezeigt.

3. Legen Sie die Serveroptionen fest.

   Hostadresse

   Geben Sie die auflösbare IP-Adresse oder einen auflösbaren Pfad und Maschinennamen ein.

   Vorhandenen Benutzer verwenden

   Aktivieren Sie dieses Feld, um einen zuvor eingegebenen Benutzernamen und ein zuvor eingegebenes Kennwort für den Provider auszuwählen.

   Benutzername

   Geben Sie Ihren Benutzernamen für den Provider an. Wenn Sie einen SQL-Server eingeben, folgt die Benutzeridentität dem Standardformat *Domäne**Name*, wenn die virtuelle Maschine einer Domäne zugeordnet ist. Das Format *lokaler_Administrator* wird verwendet, wenn der Benutzer ein lokaler Administrator ist.

   Kennwort

   Geben Sie Ihr Kennwort für den Provider ein.

   Betriebssystemtyp

   Wählen Sie das Betriebssystem des Anwendungsservers aus.
4. Klicken Sie auf **Speichern**.

Kapitel 11. IBM Spectrum Protect Plus-Systemumgebung konfigurieren und verwalten

Das Systemmanagement umfasst die folgenden Tasks: Sicherungsspeicher hinzufügen, Sites verwalten, LDAP- (Lightweight Directory Access Protocol) oder SMTP-Server (Simple Mail Transfer Protocol) registrieren sowie Schlüssel und Zertifikate für Cloudressourcen verwalten.

Die Verwaltung umfasst die folgenden Tasks: Konfiguration der virtuellen IBM Spectrum Protect Plus-Appliance überprüfen, Protokolldateien für die Fehlerbehebung erfassen und SSL-Zertifikate verwalten.

IBM Spectrum Protect Plus wird in der Regel in einer virtuellen Appliance installiert. Die virtuelle Appliance enthält die Anwendung und den Bestand. Verwaltungstasks werden in vSphere Client, mithilfe der IBM Spectrum Protect Plus-Befehlszeile oder in einer webbasierten Managementkonsole ausgeführt.

Verwaltungstasks werden von einem Systemadministrator ausgeführt. Ein Systemadministrator ist in der Regel ein Benutzer in leitender Funktion, der die vSphere- und ESX-Infrastruktur konzipiert oder implementiert hat, oder ein Benutzer mit Kenntnissen in IBM Spectrum Protect Plus, VMware und Linux-Befehlszeilenverwendung.

Infrastrukturaktualisierungen werden von IBM Aktualisierungsfunktionen gesteuert. Die Verwaltungskonsole dient als primäre Methode zur Aktualisierung der IBM Spectrum Protect Plus-Funktionen und der zugrunde liegenden Infrastrukturkomponenten, einschließlich Betriebssystem und Dateisystem. ZFS-Aktualisierungspakete (ZFS = Z File System) werden auch für vSnap-Standalone-Instanzen bereitgestellt.

Achtung: Die zugrunde liegenden Komponenten von IBM Spectrum Protect Plus dürfen Sie nur mit den von IBM bereitgestellten Aktualisierungsfunktionen aktualisieren.

Sekundären Sicherungsspeicher verwalten

Der vSnap-Server ist die primäre Sicherungsposition für Momentaufnahmen. Alle IBM Spectrum Protect Plus-Umgebungen verfügen über mindestens einen vSnap-Server. Wahlweise können Sie Momentaufnahmen aus einem vSnap-Server in ein Cloudspeichersystem oder auf einen Repository-Server auslagern.

Informationen zum Auslagern von Momentaufnahmedaten in sekundären Speicher finden Sie in „In sekundären Sicherungsspeicher auslagern” auf Seite 6.

Cloudspeicher verwalten

Für längerfristigen Datenschutz ist eine Auslagerung in den Cloudspeicher möglich.

Amazon S3-Cloudspeicher als Sicherungsspeicherprovider hinzufügen

Fügen Sie Amazon S3-Cloudspeicher hinzu, um IBM Spectrum Protect Plus die Auslagerung von Daten in S3 zu ermöglichen.

Vorbereitende Schritte

Konfigurieren Sie den Schlüssel, der für das Cloudobjekt erforderlich ist. Anweisungen finden Sie in „Zugriffsschlüssel hinzufügen” auf Seite 281.

Stellen Sie sicher, dass Cloudspeicherbuckets für die IBM Spectrum Protect Plus-Daten erstellt wurden, bevor Sie den Cloudspeicher in den folgenden Schritten hinzufügen. Informationen zum Erstellen von Buckets finden Sie in Amazon Simple Storage Service - Dokumentation.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Amazon S3-Cloudspeicher als Sicherungsspeicherprovider hinzuzufügen:

1. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud**.

© Copyright IBM Corp. 2017, 2019

2. Klicken Sie auf **Cloud hinzufügen**.
3. Wählen Sie in der Liste **Provider** den Eintrag **Amazon S3** aus.
4. Füllen Sie die Felder im Fenster **Cloudregistrierung** aus:

   Name
   Geben Sie einen aussagekräftigen Namen ein, um den Cloudspeicher zu identifizieren.

   Region
   Wählen Sie den regionalen AWS-Endpunkt (AWS = Amazon Web Services) des Cloudspeichers aus.

   Vorhandenen Schlüssel verwenden
   Aktivieren Sie dieses Feld, um einen zuvor eingegebenen Schlüssel für den Speicher auszuwählen, und wählen Sie dann den Schlüssel aus der Liste **Schlüssel auswählen** aus.

   Wenn Sie diese Option nicht auswählen, füllen Sie die folgenden Felder aus, um einen Schlüssel hinzuzufügen:

   Schlüsselname
   Geben Sie einen aussagekräftigen Namen ein, um den Schlüssel zu identifizieren.

   Zugriffsschlüssel
   Geben Sie den AWS-Zugriffsschlüssel ein. Zugriffsschlüssel werden mithilfe der AWS-Verwaltungskonsole erstellt.

   Geheimer Schlüssel
   Geben Sie den geheimen AWS-Schlüssel ein. Geheime Schlüssel werden mithilfe der AWS-Verwaltungskonsole erstellt.
5. Klicken Sie auf **Buckets abrufen** und wählen Sie dann ein Bucket aus, das als Auslagerungsziel dienen soll.

   Nachdem die Buckets generiert wurden, werden die Felder **Auslagerungsbucket** und **Archivierungsbucket** angezeigt.
6. Wählen Sie im Feld **Auslagerungsbucket** ein Bucket aus, das als Auslagerungsziel dienen soll.
7. Optional: Wählen Sie im Feld **Archivierungsbucket** eine Cloudspeicherressource aus, die als Archivierungsziel dienen soll.

   Beim Archivieren von Daten wird eine vollständige Datenkopie erstellt; das Archivieren von Daten kann außerdem Vorteile hinsichtlich längerfristigem Schutz, Kosten und Sicherheit bieten. Weitere Informationen zum Archivieren von Daten liefern die Informationen zum Kopieren von Daten in Cloudarchivierungsspeicher in „In sekundären Sicherungsspeicher auslagern” auf Seite 6.
8. Klicken Sie auf **Registrieren**.

   Der Cloudspeicher wird der Tabelle mit den Cloud-Servern hinzugefügt.

Nächste Schritte
Führen Sie die folgende Aktion aus, nachdem Sie den S3-Speicher hinzugefügt haben:

Aktion	Vorgehensweise
Ordnen Sie dem Cloudspeicher die SLA-Richtlinie zu, die für den Sicherungsjob verwendet wird.	Um eine SLA-Richtlinie zu erstellen, lesen Sie die Informationen in „SLA-Richtlinie erstellen” auf Seite 93. Um eine vorhandene SLA-Richtlinie zu ändern, lesen Sie die Informationen in „SLA-Richtlinie editieren” auf Seite 97.

IBM Cloud Object Storage als Sicherungsspeicherprovider hinzufügen
Fügen Sie IBM Cloud Object Storage hinzu, um IBM Spectrum Protect Plus die Auslagerung von Daten in die IBM Cloud zu ermöglichen.

Vorbereitende Schritte

Konfigurieren Sie den Schlüssel und das Zertifikat, die für das Cloudobjekt erforderlich sind. Anweisungen finden Sie in „Zugriffsschlüssel hinzufügen" auf Seite 281 und „Zertifikat hinzufügen" auf Seite 282.

Stellen Sie sicher, dass Cloudspeicherbuckets für die IBM Spectrum Protect Plus-Daten erstellt wurden, bevor Sie den Cloudspeicher in den folgenden Schritten hinzufügen. Informationen zum Erstellen von Buckets finden Sie in About IBM Cloud Object Storage.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um IBM Cloud Object Storage als Sicherungsspeicherprovider hinzuzufügen:

1. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud**.
2. Klicken Sie auf **Cloud hinzufügen**.
3. Wählen Sie in der Liste **Provider** den Eintrag **IBM Cloud Object Storage** aus.
4. Füllen Sie die Felder im Fenster **Cloudregistrierung** aus:

   Name
   Geben Sie einen aussagekräftigen Namen ein, um den Cloudspeicher zu identifizieren.

   Endpunkt
   Wählen Sie den Endpunkt des Cloudspeichers aus.

   Vorhandenen Schlüssel verwenden
   Aktivieren Sie dieses Feld, um einen zuvor eingegebenen Schlüssel für den Speicher auszuwählen, und wählen Sie dann den Schlüssel aus der Liste **Schlüssel auswählen** aus.

   Wenn Sie diese Option nicht auswählen, füllen Sie die folgenden Felder aus, um einen Schlüssel hinzuzufügen:

   Schlüsselname
   Geben Sie einen aussagekräftigen Namen ein, um den Schlüssel zu identifizieren.

   Zugriffsschlüssel
   Geben Sie den Zugriffsschlüssel ein.

   Geheimer Schlüssel
   Geben Sie den geheimen Schlüssel ein.

   Zertifikat
   Wählen Sie eine Methode aus, um der Ressource ein Zertifikat zuzuordnen:

   Hochladen
   Wählen Sie diese Methode aus und klicken Sie auf **Durchsuchen**, um nach dem Zertifikat zu suchen, und klicken Sie dann auf **Hochladen**.

   Kopieren und einfügen
   Wählen Sie diese Methode aus, um den Namen des Zertifikats einzugeben und den Inhalt des Zertifikats zu kopieren und einzufügen. Klicken Sie dann auf **Erstellen**.

   Vorhandenes verwenden
   Wählen Sie diese Methode aus, um ein zuvor hochgeladenes Zertifikat zu verwenden.

   Ein Zertifikat ist nicht erforderlich, wenn Sie öffentlichen IBM Cloud Object Storage hinzufügen.
5. Klicken Sie auf **Buckets abrufen** und wählen Sie dann ein Bucket aus, das als Auslagerungsziel dienen soll.

   Nachdem die Buckets generiert wurden, werden die Felder **Auslagerungsbucket** und **Archivierungsbucket** angezeigt.
6. Wählen Sie im Feld **Auslagerungsbucket** ein Bucket aus, das als Auslagerungsziel dienen soll.
7. Optional: Wählen Sie im Feld **Archivierungsbucket** eine Cloudspeicherressource aus, die als Archivierungsziel dienen soll.

   Beim Archivieren von Daten wird eine vollständige Datenkopie erstellt; das Archivieren von Daten kann außerdem Vorteile hinsichtlich längerfristigem Schutz, Kosten und Sicherheit bieten. Weitere Informa-

tionen zum Archivieren von Daten liefern die Informationen zum Kopieren von Daten in Cloudarchivierungsspeicher in „In sekundären Sicherungsspeicher auslagern” auf Seite 6.

8. Klicken Sie auf **Registrieren**.

   Der Cloudspeicher wird der Tabelle mit den Cloud-Servern hinzugefügt.

Nächste Schritte

Führen Sie die folgende Aktion aus, nachdem Sie den IBM Cloud Object Storage hinzugefügt haben:

Aktion	Vorgehensweise
Ordnen Sie dem Cloudspeicher die SLA-Richtlinie zu, die für den Sicherungsjob verwendet wird.	Um eine SLA-Richtlinie zu erstellen, lesen Sie die Informationen in „SLA-Richtlinie erstellen” auf Seite 93. Um eine vorhandene SLA-Richtlinie zu ändern, lesen Sie die Informationen in „SLA-Richtlinie editieren” auf Seite 97.

Microsoft Azure-Cloudspeicher als Sicherungsspeicherprovider hinzufügen

Fügen Sie Microsoft Azure-Cloudspeicher hinzu, um IBM Spectrum Protect Plus die Auslagerung von Daten in den Microsoft Azure-Blob-Speicher zu ermöglichen.

Vorbereitende Schritte

Stellen Sie sicher, dass Cloudspeicherbuckets für die IBM Spectrum Protect Plus-Daten erstellt wurden, bevor Sie den Cloudspeicher in den folgenden Schritten hinzufügen. Informationen zum Erstellen von Buckets finden Sie in der Azure-Dokumentation.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Microsoft Azure-Cloudspeicher als Sicherungsspeicherprovider hinzuzufügen:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud**.
2. Klicken Sie auf **Cloud hinzufügen**.
3. Wählen Sie in der Liste **Provider** den Eintrag **Microsoft Azure-Blob-Speicher** aus.
4. Füllen Sie die Felder im Fenster **Cloudregistrierung** aus:

   Name
   Geben Sie einen aussagekräftigen Namen ein, um den Cloudspeicher zu identifizieren.

   Endpunkt
   Wählen Sie den Endpunkt des Cloudspeichers aus.

   Vorhandenen Schlüssel verwenden
   Aktivieren Sie dieses Feld, um einen zuvor eingegebenen Schlüssel für den Speicher auszuwählen, und wählen Sie dann den Schlüssel aus der Liste **Schlüssel auswählen** aus.

   Wenn Sie diese Option nicht auswählen, füllen Sie die folgenden Felder aus, um einen Schlüssel hinzuzufügen:

   Schlüsselname
   Geben Sie einen aussagekräftigen Namen ein, um den Schlüssel zu identifizieren.

   Name des Speicheraccounts
   Geben Sie den Namen des Microsoft Azure-Zugriffsspeicheraccounts ein. Dieser stammt aus dem Azure-Verwaltungsportal.

   Gemeinsam genutzter Schlüssel für Speicheraccount
   Geben Sie den Microsoft Azure-Schlüssel aus einem der Schlüsselfelder im Azure-Verwaltungsportal ein (Schlüssel1 oder Schlüssel2).

5. Klicken Sie auf **Buckets abrufen** und wählen Sie dann ein Bucket aus, das als Auslagerungsziel dienen soll.

   Nachdem die Buckets generiert wurden, werden die Felder **Auslagerungsbucket** und **Archivierungsbucket** angezeigt.
6. Wählen Sie im Feld **Auslagerungsbucket** ein Bucket aus, das als Auslagerungsziel dienen soll.
7. Optional: Wählen Sie im Feld **Archivierungsbucket** eine Cloudspeicherressource aus, die als Archivierungsziel dienen soll.

   Beim Archivieren von Daten wird eine vollständige Datenkopie erstellt; das Archivieren von Daten kann außerdem Vorteile hinsichtlich längerfristigem Schutz, Kosten und Sicherheit bieten. Weitere Informationen zum Archivieren von Daten liefern die Informationen zum Kopieren von Daten in Cloudarchivierungsspeicher in „In sekundären Sicherungsspeicher auslagern" auf Seite 6.
8. Klicken Sie auf **Registrieren**.

   Der Cloudspeicher wird der Tabelle mit den Cloud-Servern hinzugefügt.

Nächste Schritte

Führen Sie die folgende Aktion aus, nachdem Sie den Microsoft Azure-Speicher hinzugefügt haben:

Aktion	Vorgehensweise
Ordnen Sie dem Cloudspeicher die SLA-Richtlinie zu, die für den Sicherungsjob verwendet wird.	Um eine SLA-Richtlinie zu erstellen, lesen Sie die Informationen in „SLA-Richtlinie erstellen" auf Seite 93. Um eine vorhandene SLA-Richtlinie zu ändern, lesen Sie die Informationen in „SLA-Richtlinie editieren" auf Seite 97.

Einstellungen für Cloudspeicher editieren

Editieren Sie die Einstellungen für einen Cloudspeicherprovider, um Änderungen in Ihrer Cloudumgebung widerzuspiegeln.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Cloudspeicherprovider zu editieren:

1. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud**.
2. Klicken Sie auf das Symbol für Editieren , das einem Cloud-Provider zugeordnet ist.

   Das Fenster **Cloud aktualisieren** wird angezeigt.
3. Überarbeiten Sie die Einstellungen für den Cloud-Provider und klicken Sie dann auf **Aktualisieren**.

Cloudspeicher löschen

Löschen Sie einen Cloudspeicherprovider, um Änderungen in Ihrer Cloudumgebung widerzuspiegeln. Stellen Sie sicher, dass der Provider keinen SLA-Richtlinien zugeordnet ist, bevor Sie den Provider löschen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Cloudspeicherprovider zu löschen:

1. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **Sicherungsspeicher** > **Cloud**.
2. Klicken Sie auf das Symbol für Löschen , das einem Provider zugeordnet ist.
3. Klicken Sie auf **Ja**, um den Provider zu löschen.

Speicher des Repository-Servers verwalten

Für längerfristigen Datenschutz ist eine Auslagerung auf einen Repository-Server möglich. Für das aktuelle Release von IBM Spectrum Protect Plus muss der Repository-Server ein IBM Spectrum Protect-Server

der Version 8.1.7 oder höher sein. Für die Archivierung auf Band ist IBM Spectrum Protect-Server Version 8.1.8 oder höher erforderlich.

IBM Spectrum Protect-Server-Server als Auslagerungsziel konfigurieren
Um Daten auf einen IBM Spectrum Protect-Server auslagern zu können, müssen Sie zuerst IBM Spectrum Protect Plus als einen Objektclient für den Server konfigurieren.

Informationen zu diesem Vorgang

Nach der Konfiguration eines Objektclients werden Schlüssel und ein Zertifikat zur Verfügung gestellt, um eine sichere Verbindung zum IBM Spectrum Protect-Server zu ermöglichen. Diese Elemente sind erforderlich, um den Repository-Server in IBM Spectrum Protect Plus hinzufügen zu können.

Um den Objektclient hinzuzufügen, müssen Sie mit der IBM Spectrum Protect-Server-Umgebung vertraut sein und Erfahrungen im Umgang mit dem Operations Center oder den Verwaltungsbefehlen des IBM Spectrum Protect-Servers haben. Wenn Sie Unterstützung benötigen, wenden Sie sich an Ihren IBM Spectrum Protect-Administrator.

IBM Spectrum Protect Plus erkennt Auslagerungen an den IBM Spectrum Protect-Server, erkennt aber keine nachfolgenden Replikationsoperationen des IBM Spectrum Protect-Servers.

Die Dokumentation zum Konfigurieren von IBM Spectrum Protect als Auslagerungsziel ist im IBM Knowledge Center verfügbar und kann wie folgt abgerufen werden:

- Eine Übersicht über den Konfigurationsprozess finden Sie in Daten aus IBM Spectrum Protect Plus auslagern.
- Voraussetzungen für den Auslagerungsprozess finden Sie in Auslagerung von Daten aus IBM Spectrum Protect Plus vorbereiten.
- Informationen zum Betriebssystem AIX finden Sie in Daten für die Auslagerung in AIX®-Umgebungen konfigurieren.
- Informationen zu Linux- oder Windows-Betriebssystemen finden Sie in Daten für die Auslagerung in Linux- und Windows-Umgebungen konfigurieren.
- Eine Übersicht über den Konfigurationsprozess finden Sie in Daten aus IBM Spectrum Protect Plus auslagern.
- Voraussetzungen für den Auslagerungsprozess finden Sie in Auslagerung von Daten aus IBM Spectrum Protect Plus vorbereiten.
- Informationen zum Betriebssystem AIX finden Sie in Daten für die Auslagerung in AIX®-Umgebungen konfigurieren.
- Informationen zu Linux- oder Windows-Betriebssystemen finden Sie in Daten für die Auslagerung in Linux- und Windows-Umgebungen konfigurieren.

Zugehörige Tasks
„Repository-Server als Sicherungsspeicherprovider hinzufügen” auf Seite 279
Fügen Sie einen Repository-Server hinzu, um IBM Spectrum Protect Plus die Auslagerung von Daten auf den Server zu ermöglichen.

Auslagerung von Daten aus IBM Spectrum Protect Plus vorbereiten
Bevor Daten aus IBM Spectrum Protect Plus in IBM Spectrum Protect ausgelagert werden, führen Sie die Vorbereitungsschritte in der IBM Spectrum Protect-Umgebung aus.

Vorgehensweise

1. Stellen Sie sicher, dass Sie einen IBM Spectrum Protect-Server-Port zu dem IBM Spectrum Protect Plus-Objektclient öffnen können, der für die Datenauslagerungsoperationen verwendet werden soll. Die Standardportnummer ist 9000. Wenn zwischen dem Objektclient und dem Objektagenten Firewalls vorhanden sind, konfigurieren Sie den Objektagenten für den Zugriff auf den entsprechenden Port durch die Firewall.

2. Überprüfen Sie die Einstellungen für die Maßnahmendomäne, die für Datenauslagerungsoperationen verwendet werden soll. Ein Objektclientknoten wird dieser Maßnahmendomäne zugeordnet, wenn der Knoten mit dem Verwaltungsbefehl **REGISTER NODE** oder **UPDATE NODE** des IBM Spectrum Protect-Servers registriert bzw. aktualisiert wird.

   Bei der Angabe von Maßnahmendomänen für IBM Spectrum Protect Plus-Auslagerungsoperationen gelten die folgenden Voraussetzungen:

   - Die Domäne, der der Knoten zugeordnet ist, muss über eine Sicherungskopiengruppe verfügen. Objekte, die in einem Objektclientknoten gespeichert werden, sind immer Sicherungsobjekte. Eine Archivierungskopiengruppe ist nicht erforderlich.
   - Sie müssen einen Containerspeicherpool verwenden. Der Speicherpool, der im `Kopienziel` der Kopiengruppe angegeben ist, muss entweder ein Verzeichniscontainer- oder Cloud-Containerspeicherpool sein.
   - Alle Objekte haben eindeutige Namen. Da keine inaktiven Versionen von Objekten vorhanden sind, können Sie das Feld `Versionen bestehender Daten` auf 1 setzen.
   - Da Sicherungskopiengruppen nur aktive Versionen enthalten, können Sie die Felder `Extraversionen aufbewahren` und `Einzige Version aufbewahren` auf 0 setzen.
   - Der IBM Spectrum Protect-Server steuert, zu welchem Zeitpunkt Objekte gelöscht werden. Stellen Sie sicher, dass dem Objektclientknoten das Löschen von Sicherungskopiengruppen erlaubt ist.

Beispiel: Detaillierte Informationen zu einer Maßnahmendomäne für eine IBM Spectrum Protect Plus-Auslagerungsoperation anzeigen

Einstellungen für eine Kopiengruppe für einen Objektclientknoten anzeigen

```
query copygroup format=detailed
```

```
               Name der Maßnahmendomäne: TAPSRV03_OBJECT
                    Name der Maßnahmengruppe: SET1
                 Name der Verwaltungsklasse: BACK_DISK
                      Name der Kopiengruppe: STANDARD
                           Kopiengruppenart: Sicherung
                  Versionen bestehender Daten: 1
                   Versionen gelöschter Daten: 0
                   Extraversionen aufbewahren: 0
                  Einzige Version aufbewahren: 0
                                Kopienmodus: Geändert
                          Kopiennummerierung: Gemeinsam statisch
                            Kopienhäufigkeit: 0
                                  Kopienziel: DEDUPPOOL
                  Ziel für Inhaltsverzeichnis:
    Letzte Aktualisierung durch (Administrator): JBASIL
          Datum/Zeit der letzten Aktualisierung: 17.01.2019 14:38:05
                             Verwaltendes Profil:
                            Änderungen anstehend: Nein
```

Daten auf AIX-Systeme auslagern

Sie können Daten aus IBM Spectrum Protect Plus auf einen IBM Spectrum Protect-Server unter AIX auslagern.

Informationen zu diesem Vorgang

Ein IBM Spectrum Protect-Objektagent kann nicht direkt unter einem IBM AIX-Betriebssystem ausgeführt werden. Sie können jedoch IBM Spectrum Protect Plus-Daten auf einen IBM Spectrum Protect-Objektclient auf einem AIX-System auslagern, indem Sie zunächst einen Objektagenten unter einem Linux x86_64-Betriebssystem konfigurieren. Der eigenständige Objektagent ist nur unter dem Linux x86_64-Betriebssystem verfügbar.

Nachdem der IBM Spectrum Protect Plus-Objektclient Daten an den IBM Spectrum Protect-Objektagenten unter Linux x86_64 gesendet hat, überträgt der Objektagent Daten auf einen IBM Spectrum Protect-Objektclient unter AIX.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Daten aus IBM Spectrum Protect Plus auf einen IBM Spectrum Protect-Server unter AIX auszulagern:

1. Geben Sie auf dem AIX-Server den folgenden Verwaltungsbefehl des IBM Spectrum Protect-Servers aus:

   ```
   setopt EnableAIXS3Interface Yes
   ```

2. Definieren Sie auf dem AIX-Server einen Objektagenten, indem Sie den folgenden Verwaltungsbefehl des IBM Spectrum Protect-Servers ausgeben. Um die Adresse der höheren Ebene (HLA) und die Adresse der unteren Ebene (LLA) zu definieren, verwenden Sie die IP-Adresse des Hostsystems und den Port, die bzw. der vom Objektagenten verwendet wird.

   ```
   define server Name_des_Objektagenten
   hla=IP-Adresse_des_Hostsystems_des_Objektagenten
   lla=Port_des_Objektagenten objectagent=yes
   ```

   Tipp: Der Standardwert für den Port des Objektagenten ist 9000. Wird bereits ein lokaler Objektagent auf dem System ausgeführt, muss der Objektagent, der für den AIX-Server konfiguriert wird, eine andere Portnummer als der vorhandene Objektagent verwenden.

3. Laden Sie die folgenden Scripts auf das Hostsystem des Objektagenten herunter:

   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/startObjectAgent.sh
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent.rc
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/spObjectAgent.rc.u
   - ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/objectagent/v8r1/Linux/8.1.7.000/x86_64/delObjectAgentSvc.sh

   Auf dem Hostsystem des Objektagenten kann entweder IBM Spectrum Protect Plus oder ein IBM Spectrum Protect-Server installiert sein.

   Wenn der IBM Spectrum Protect-Server installiert ist, können Sie die Datei `spObjectAgent` im Serververzeichnis verwenden und müssen den Agenten und seine Scripts nicht erneut herunterladen.

4. Stellen Sie sicher, dass die folgenden Dateien über Berechtigungen zur Ausführung verfügen:

   - `spObjectAgent`
   - `startObjectAgent.sh`
   - `spObjectAgent.rc`
   - `spObjectAgent.rc.u`
   - `delObjectAgentSvc.sh`

5. Kopieren Sie auf dem AIX-Serversystem die folgenden beiden Elemente in ein Verzeichnis auf dem Hostsystem des Objektagenten unter Linux:

   - Objektagentenservervzeichnis
   - Öffentliches Serverzertifikat

   Das Objektagentenserververzeichnis wurde beim Ausführen des Befehls **DEFINE SERVER** erstellt. Das Verzeichnis umfasst die folgende Datei und die folgenden Zertifikate:

   - Eine Konfigurationsdatei zum Erstellen und Starten eines Objektagentenservice
   - Zertifikate für die Kommunikation zwischen dem Objektagenten und dem Server

Das Objektagentenserververzeichnis wird im Serverinstanzverzeichnis erstellt: */Ausgangsverzeichnis_der_Serverinstanz/Name_des_Objektagenten*. Beispiel:

`/home/tsminst1/OBJAGENT1`

Das öffentliche Serverzertifikat (`cert256.arm`) befindet sich normalerweise im Serverinstanzverzeichnis.

6. Lokalisieren Sie im Objektagentenserververzeichnis, das im vorherigen Schritt kopiert wurde, die Konfigurationsdatei für den Objektagenten (`spObjectAgent_`*Name_des_Objektagenten_Server-Port*`.config`).

   Beispiel: `spObjectAgent_OBJAGENT1_1500.config`

   Aktualisieren Sie in der Konfigurationsdatei die Speicherpositionen der folgenden Dateien. Beispiel:

   ```
   objagentexe=\"/opt/tivoli/tsm/server/bin/spObjectAgent\"
      keystore="/home/tsminst1/OBJAGENT1/agentcert.p12"
      pwdfile="/home/tsminst1/OBJAGENT1/agentcert.pwd"
      serverkeypub="/home/tsminst1/OBJAGENT1/cert256.arm"
      agentconfig=\"/home/tsminst1/OBJAGENT1/spObjectAgent_OBJAGENT1_1500.config\"
   ```

7. Überschreiben Sie den Parameter **SERVERHLA** in der Konfigurationsdatei für den Objektagenten mit der IP-Adresse des AIX-Servers:

   ```
   serverhla=IP-Adresse_des_AIX-Servers
   ```

   Tipp: Der Objektagent verwendet diesen Wert zum Lokalisieren des IBM Spectrum Protect-Servers.

8. Um den Objektagenten auf dem Hostsystem zu erstellen und zu starten, führen Sie das Script `startObjectAgent.sh` mit der Konfigurationsdatei aus:

   ```
   startObjectAgent.sh spObjectAgent_Name_des_Objektagenten_Server-Port.config
   ```

9. Registrieren Sie einen Objektagentenclient auf dem AIX-Server, indem Sie den folgenden IBM Spectrum Protect-Serverbefehl ausgeben:

   ```
   register node Knotenname type=objectclient
   ```

   Wichtig: Notieren Sie die Anmelde-Benutzer-ID und das Kennwort, die bzw. das automatisch generiert wird. Sie benötigen die Berechtigungsnachweise, um die Verbindung zum Objektagenten herzustellen.

10. Um die Verbindung vom IBM Spectrum Protect Plus-Objektclient zum Objektagenten herzustellen, rufen Sie die IBM Spectrum Protect Plus-Onlinedokumentation auf und führen Sie die Anweisungen in Repository-Server als Sicherungsspeicherprovider hinzufügen aus.

Daten auf Linux- und Windows-Systeme auslagern

Sie können Daten aus IBM Spectrum Protect Plus auf einen IBM Spectrum Protect-Server unter Linux oder Windows auslagern.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Daten aus IBM Spectrum Protect Plus auf einen IBM Spectrum Protect-Server unter Linux oder Windows auszulagern:

1. Konfigurieren Sie einen Objektagenten.
   a) Klicken Sie in der Menüleiste des Operations Center auf **Server**.
   b) Wählen Sie eine Serverzeile aus und klicken Sie auf **Details**.
   c) Wählen Sie im linken Navigationsfenster **Objektagent** aus und führen Sie die Schritte zum Erstellen eines Objektagenten und zum Starten eines Objektagentenservice aus. Verwenden Sie für die Authentifizierung beim Objektagenten das generierte Zertifikat.

   Tipp: Verwenden Sie alternativ den Verwaltungsbefehl **DEFINE SERVER** des IBM Spectrum Protect-Servers, um einen Objektagenten zu erstellen. Geben Sie `OBJECTAGENT=YES` an. Schließen Sie die

Konfiguration ab, indem Sie einen Objektagentenservice auf dem System starten, auf dem sich der IBM Spectrum Protect-Server befindet.

2. Konfigurieren Sie einen Objektclient.

   Tipp: Wenn Sie einen Objektclient erstellen, bevor Sie den zugehörigen Objektagenten erstellen, erzwingt der Assistent 'Client hinzufügen' die Erstellung des Objektagenten.

   a) Klicken Sie in der Menüleiste des Operations Center auf **Clients**.

   b) Klicken Sie in der Tabelle 'Clients' auf **+Client**.

   c) Wählen Sie 'Objektclient' aus und führen Sie die Anweisungen im Assistenten **Client hinzufügen** aus.

   Nachdem die Schritte im Assistenten abgeschlossen sind, werden Ihnen der Endpunkt für die Kommunikation mit dem Objektagenten auf dem Server sowie die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel zum Herstellen einer sicheren Verbindung zur Verfügung gestellt. Wenn IBM Spectrum Protect Plus als ein Objektclient verwendet wird, muss es seine Anforderungen an den Endpunkt übertragen und die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel verwenden.

   Tipp: Verwenden Sie alternativ den Befehl **REGISTER NODE**, um einen Objektclient zu erstellen. Geben Sie TYPE=OBJECTCLIENT an.

Objektagentenservice löschen

Wenn ein Objektagent vom IBM Spectrum Protect-Server gelöscht wird, muss der Objektagentenservice vom Hostsystem gelöscht werden. Um den Löschprozess für einen Objektagenten auszuführen, löschen Sie den zugehörigen Service.

Vorbereitende Schritte

Um den Objektagentenservice auf einem Linux-Betriebssystem zu löschen, müssen Sie das Script `delObjectAgentSvc.sh` mit der Konfigurationsdatei für den Objektagenten ausführen. Stellen Sie sicher, dass Sie sich mit der Rootbenutzer-ID beim Hostsystem des Objektagenten anmelden können.

Um den Objektagentenservice auf einem Windows-Betriebssystem zu löschen, müssen Sie die Stapeldatei `delObjectAgentSvc.cmd` mit der Konfigurationsdatei für den Objektagenten ausführen. Stellen Sie sicher, dass Sie über Windows-Administratorberechtigungen für die Anmeldung beim Hostsystem des Objektagenten verfügen.

Vorgehensweise

1. Überprüfen Sie, ob der Objektagent vom IBM Spectrum Protect-Server gelöscht wurde, indem Sie den Serververwaltungsbefehl **QUERY SERVER** ausgeben.
2. Öffnen Sie eine Befehlszeile.
3. Geben Sie den folgenden Befehl in einer einzigen Zeile aus. In den Beispielen werden die Serverstandardverzeichnisse verwendet.

   Linux

   ```
   /opt/tivoli/tsm/server/bin/delObjectAgentSvc.sh
   /Konfigurationspfad_des_Objektagenten/spObjectAgent_Name_des_Objektagenten_Server-Port.config
   ```

   Windows

   ```
   "C:\Programme\Tivoli\TSM\server\delObjectAgentSvc.cmd"
   "Konfigurationspfad_des_Objektagenten\spObjectAgent_Name_des_Objektagenten_Server-Port.con
   fig"
   ```

   Dabei gilt Folgendes:

   Konfigurationspfad_des_Objektagenten

   Gibt den Konfigurationspfad für den Objektagenten an.

Name_des_Objektagenten

Gibt den Namen des Objektagenten an.

Server-Port

Gibt die Portnummer des IBM Spectrum Protect-Servers an.

Repository-Server als Sicherungsspeicherprovider hinzufügen
Fügen Sie einen Repository-Server hinzu, um IBM Spectrum Protect Plus die Auslagerung von Daten auf den Server zu ermöglichen.

Vorbereitende Schritte

Konfigurieren Sie den Schlüssel und das Zertifikat, die für den Repository-Server erforderlich sind. Anweisungen finden Sie in „Zugriffsschlüssel hinzufügen" auf Seite 281 und „Zertifikat hinzufügen" auf Seite 282.

Für das aktuelle Release von IBM Spectrum Protect Plus muss der Repository-Server ein IBM Spectrum Protect-Server sein.

Konfigurieren Sie IBM Spectrum Protect Plus als einen Objektclient für den IBM Spectrum Protect-Server. Der Objektclientknoten überträgt und speichert ausgelagerte Daten. Nachdem die Konfigurationsprozedur abgeschlossen ist, stellt Ihnen der Assistent den Endpunkt für die Kommunikation mit dem Objektagenten auf dem Server sowie die Zugriffs-ID, den geheimen Schlüssel und das Zertifikat zum Herstellen einer sicheren Verbindung zur Verfügung. „IBM Spectrum Protect-Server-Server als Auslagerungsziel konfigurieren" auf Seite 274.

Zertifikate können aus dem Operations Center des IBM Spectrum Protect-Servers abgerufen werden, indem zu dem folgenden Fenster navigiert wird: **Server** > **Objektagent** > **Agentenzertifikat**. Es ist auch möglich, das Zertifikat von der IBM Spectrum Protect Plus-Appliance abzurufen, indem der folgende Befehl ausgeführt wird: `openssl s_client -showcerts -connect <IP-Adresse>:9000 </dev/null 2>/dev/null | openssl x509`

Aufbewahrungseinstellungen für Auslagerungen werden vollständig über zugeordnete SLA-Richtlinien in IBM Spectrum Protect Plus gesteuert. Aufbewahrungseinstellungen für Kopiengruppen des IBM Spectrum Protect-Servers werden nicht für Auslagerungsoperationen verwendet.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen IBM Spectrum Protect-Server als Sicherungsspeicherprovider hinzuzufügen:

1. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server**.
2. Klicken Sie auf **Repository-Server hinzufügen**.
3. Füllen Sie die Felder im Fenster **Repository-Server registrieren** aus:

   Name
   Geben Sie einen aussagekräftigen Namen ein, um den Repository-Server zu identifizieren.

   Hostname
   Geben Sie die High-Level-Adresse (HLA) des Objektagenten des Repository-Servers ein. Diese Informationen können durch Ausführen des Befehls IBM Spectrum Protect `q serv OBJAGENT f=d` abgerufen werden.

   Port
   Geben Sie den Kommunikationsport des Repository-Servers an.

   Vorhandenen Schlüssel verwenden
   Aktivieren Sie dieses Feld, um einen zuvor eingegebenen Schlüssel für das Repository auszuwählen, und wählen Sie dann den Schlüssel aus der Liste **Schlüssel auswählen** aus.

   Wenn Sie diese Option nicht auswählen, füllen Sie die folgenden Felder aus, um einen Schlüssel hinzuzufügen:

Schlüsselname
Geben Sie einen aussagekräftigen Namen ein, um den Schlüssel zu identifizieren.

Zugriffsschlüssel
Geben Sie den Zugriffsschlüssel ein.

Geheimer Schlüssel
Geben Sie den geheimen Schlüssel ein.

Zertifikat
Wählen Sie eine Methode aus, um der Ressource ein Zertifikat zuzuordnen. Wenn das Zertifikat kopiert wird, müssen die Textzeilen BEGIN und END eingeschlossen werden.

Hochladen
Wählen Sie diese Methode aus und klicken Sie auf **Durchsuchen**, um nach dem Zertifikat zu suchen, und klicken Sie dann auf **Hochladen**.

Kopieren und einfügen
Wählen Sie diese Methode aus, um den Namen des Zertifikats einzugeben und den Inhalt des Zertifikats zu kopieren und einzufügen; klicken Sie dann auf **Erstellen**.

Vorhandenes verwenden
Wählen Sie diese Methode aus, um ein zuvor hochgeladenes Zertifikat zu verwenden.

4. Klicken Sie auf **Registrieren**.
   Der IBM Spectrum Protect-Server wird der Tabelle der Repository-Server hinzugefügt.

Nächste Schritte

Führen Sie die folgende Aktion aus, nachdem Sie einen Repository-Server hinzugefügt haben:

Aktion	Vorgehensweise
Ordnen Sie dem Repository-Server die SLA-Richtlinie zu, die für den Sicherungsjob verwendet wird.	Informationen zum Erstellen einer SLA-Richtlinie finden Sie in „SLA-Richtlinie erstellen” auf Seite 93. Informationen zum Ändern einer vorhandenen SLA-Richtlinie finden Sie in „SLA-Richtlinie editieren” auf Seite 97.

Einstellungen für einen Repository-Server editieren

Editieren Sie die Einstellungen für einen Repository-Server-Provider, um Änderungen in Ihrer Cloudumgebung widerzuspiegeln.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Repository-Server-Provider zu editieren:

1. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server**.
2. Klicken Sie auf das Symbol für Editieren , das einem Repository-Server-Provider zugeordnet ist.
   Das Fenster **Repository-Server aktualisieren** wird angezeigt.
3. Überarbeiten Sie die Einstellungen für den Repository-Server-Provider und klicken Sie dann auf **Aktualisieren**.

Repository-Server löschen

Löschen Sie einen Repository-Server-Provider, um Änderungen in Ihrer Umgebung widerzuspiegeln. Stellen Sie sicher, dass der Provider keinen SLA-Richtlinien zugeordnet ist, bevor Sie den Provider löschen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Repository-Server-Provider zu löschen:

1. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **Sicherungsspeicher** > **Repository-Server**.
2. Klicken Sie auf das Symbol für Löschen ✕, das einem Repository-Server-Provider zugeordnet ist.
3. Klicken Sie auf **Ja**, um den Provider zu löschen.

Schlüssel und Zertifikate verwalten

Damit Cloudressourcen und Repository-Server als Auslagerungsziel genutzt werden können, sind Berechtigungsnachweise erforderlich. Zugriffsschlüssel und geheime Schlüssel werden von Ihrer Cloudressourcen- oder Repository-Server-Schnittstelle bereitgestellt. Diese Schlüssel dienen als Benutzername und Kennwort Ihrer Auslagerungsziele und ermöglichen den Zugriff auf diese Ziele durch IBM Spectrum Protect Plus. Bei einigen Auslagerungszielen sind aus Gründen der zusätzlichen Datensicherheit außerdem Zertifikate erforderlich.

Wenn Sie eine Ressource in IBM Spectrum Protect Plus einsetzen, die Berechtigungsnachweise für den Zugriff auf ein Auslagerungsziel erforderlich macht, wählen Sie **Vorhandenen Schlüssel verwenden** oder **Vorhandenes Zertifikat verwenden** und dann den zugehörigen Schlüssel bzw. das zugehörige Zertifikat aus.

Zugriffsschlüssel hinzufügen

Fügen Sie einen Zugriffsschlüssel hinzu, um Berechtigungsnachweise für eine Cloudressource oder einen Repository-Server bereitzustellen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Schlüssel hinzuzufügen:

1. Erstellen Sie Ihren Zugriffsschlüssel und Ihren geheimen Schlüssel über die Schnittstelle der Cloudressource oder des Repository-Servers. Notieren Sie den Zugriffsschlüssel und den geheimen Schlüssel.
2. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **Schlüssel und Zertifikate**.
3. Klicken Sie im Abschnitt **Zugriffsschlüssel** auf **Zugriffsschlüssel hinzufügen**.
4. Füllen Sie die Felder im Fenster **Schlüsseleigenschaften** aus:

   Name

   Geben Sie einen aussagekräftigen Namen ein, um den Zugriffsschlüssel zu identifizieren.

   Zugriffsschlüssel

   Geben Sie den Zugriffsschlüssel der Cloudressource oder des Repository-Servers ein. Geben Sie für Microsoft Azure den Namen des Speicheraccounts ein.

   Geheimer Schlüssel

   Geben Sie den geheimen Schlüssel der Cloudressource oder des Repository-Servers ein. Geben Sie für Microsoft Azure den Schlüssel aus einem der Schlüsselfelder ein (Schlüssel1 oder Schlüssel2).
5. Klicken Sie auf **Speichern**.

   Der Schlüssel wird in der Tabelle **Zugriffsschlüssel** angezeigt und kann ausgewählt werden, wenn eine Funktion verwendet wird, die Berechtigungsnachweise für den Zugriff auf eine Ressource mithilfe der Option **Vorhandenen Schlüssel verwenden** erfordert.

Zugriffsschlüssel löschen

Löschen Sie einen Zugriffsschlüssel, wenn er veraltet ist. Stellen Sie sicher, dass Sie der Cloudressource oder dem Repository-Server einen neuen Zugriffsschlüssel zuordnen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Zugriffsschlüssel zu löschen:

1. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **Schlüssel und Zertifikate**.

2. Klicken Sie auf das Symbol für Löschen ✕, das einem Zugriffsschlüssel zugeordnet ist.
3. Klicken Sie auf **Ja**, um den Zugriffsschlüssel zu löschen.

Zertifikat hinzufügen

Fügen Sie ein Zertifikat hinzu, um Berechtigungsnachweise für eine Cloudressource oder einen Repository-Server bereitzustellen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Zertifikat hinzuzufügen:

1. Exportieren Sie ein Zertifikat aus Ihrer Cloudressource oder von Ihrem Repository-Server.
2. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **Schlüssel und Zertifikate**.
3. Klicken Sie im Abschnitt **Zertifikate** auf **Zertifikat hinzufügen**.
4. Füllen Sie die Felder im Fenster **Zertifikatseigenschaften** aus:

   Typ

   Wählen Sie den Cloudressourcentyp oder Repository-Servertyp aus.

   Zertifikat

   Wählen Sie eine Methode aus, um das Zertifikat hinzuzufügen:

   Hochladen
   Wählen Sie diese Methode aus, um lokal nach dem Zertifikat zu suchen.

   Kopieren und einfügen
   Wählen Sie diese Methode aus, um den Namen des Zertifikats einzugeben und den Inhalt des Zertifikats zu kopieren und einzufügen.
5. Klicken Sie auf **Speichern**.

   Der Schlüssel wird in der Tabelle **Zertifikate** angezeigt und kann ausgewählt werden, wenn eine Funktion verwendet wird, die Berechtigungsnachweise für den Zugriff auf eine Ressource mithilfe der Option **Vorhandenes Zertifikat verwenden** erfordert.

Zertifikat löschen

Löschen Sie ein Zertifikat, wenn es veraltet ist. Stellen Sie sicher, dass Sie der Cloudressource oder dem Repository-Server ein neues Zertifikat zuordnen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein Zertifikat zu löschen:

1. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **Schlüssel und Zertifikate**.
2. Klicken Sie auf das Symbol für Löschen ✕, das einem Zertifikat zugeordnet ist.
3. Klicken Sie auf **Ja**, um das Zertifikat zu löschen.

SSH-Schlüssel hinzufügen

Fügen Sie einen SSH-Schlüssel hinzu, um Berechtigungsnachweise für Linux-basierte Ressourcen, einschließlich Dateiindexierungs- und -zurückschreibungsoperationen auf virtuellen Maschinen unter vCenter und Hyper-V sowie auf Oracle-, Db2- und MongoDB-Anwendungsservern, bereitzustellen. SSH-Schlüssel stellen eine sichere Verbindung zwischen Ihren Ressourcen und IBM Spectrum Protect Plus zur Verfügung.

Vorbereitende Schritte

- Der SSH-Service muss an Port 22 auf dem Server aktiv sein und alle Firewalls müssen so konfiguriert sein, dass sie IBM Spectrum Protect Plus das Herstellen der Verbindung zum Server mit SSH ermöglichen. Das Subsystem SFTP für SSH muss ebenfalls aktiviert sein.

- Stellen Sie sicher, dass der öffentliche SSH-Schlüssel für den IBM Spectrum Protect Plus-Agentenbenutzer in die entsprechende Datei authorized_keys gestellt wird. Normalerweise befindet sich die Datei an der Position /home/<Benutzername>/.ssh/authorized_keys. Die Berechtigungen für das Verzeichnis .ssh und alle Dateien unter ihm müssen auf 600 gesetzt sein.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Schlüssel hinzuzufügen:

1. Generieren Sie in Ihrer Ressource einen SSH-Schlüssel. Geben Sie beispielsweise auf einem Oracle-Server den Befehl `ssh-keygen` ein und befolgen Sie die Anweisungen.
2. Wenn Sie zur Eingabe der Datei zum Speichern des Schlüssels aufgefordert werden, geben Sie eine Datei und eine Position an, beispielsweise: `/root/sshkey`.
3. Die Datei `sshkey.pub`, die in Schritt 2 an der Position /root auf dem Server eingegeben wurde, enthält den öffentlichen Schlüssel. Dieser wird später kopiert, eingefügt und in der Datei `authorized_keys` gespeichert, nachdem `cd ~/.ssh` ausgeführt wurde, während der Benutzer bei IBM Spectrum Protect Plus angemeldet ist.
4. Klicken Sie im Navigationsfenster von IBM Spectrum Protect Plus auf **Systemkonfiguration** > **Schlüssel und Zertifikate**.
5. Klicken Sie im Abschnitt **SSH-Schlüssel** auf **SSH-Schlüssel hinzufügen**.
6. Füllen Sie die Felder im Fenster **Eigenschaften für SSH-Schlüssel** aus:

   Name

   Geben Sie einen aussagekräftigen Namen ein, um den SSH-Schlüssel zu identifizieren.

   Benutzer

   Geben Sie den Benutzer ein, der der Ressource und dem SSH-Schlüssel zugeordnet ist.

   Privater Schlüssel

   Kopieren Sie den privaten Schlüssel, der in der SSH-Schlüsseldatei enthalten ist, und fügen Sie ihn ein.
7. Klicken Sie auf **Speichern**.

   Der Schlüssel wird in der Tabelle **SSH-Schlüssel** angezeigt und kann ausgewählt werden, wenn eine Funktion verwendet wird, die Berechtigungsnachweise für den Zugriff auf eine Ressource mithilfe der Option **Schlüssel** erfordert.

SSH-Schlüssel löschen

Löschen Sie einen SSH-Schlüssel, wenn er veraltet ist. Stellen Sie sicher, dass Sie Ihren Ressourcen einen neuen SSH-Schlüssel zuordnen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen SSH-Schlüssel zu löschen:

1. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **Schlüssel und Zertifikate**.
2. Klicken Sie auf das Symbol für Löschen ✕, das einem SSH-Schlüssel zugeordnet ist.
3. Klicken Sie auf **Ja**, um den SHH-Schlüssel zu löschen.

Sites verwalten

Eine *Site* ist ein IBM Spectrum Protect Plus-Richtlinienkonstrukt, das zur Steuerung der Platzierung von Daten in einer Umgebung verwendet wird.

Eine Site kann eine physische Site, wie beispielsweise ein Datencenter, oder eine logische Site, wie beispielsweise eine Abteilung oder eine Organisation, sein. IBM Spectrum Protect Plus-Komponenten werden Sites zugeordnet, um Datenpfade einzugrenzen und zu optimieren. Eine IBM Spectrum Protect Plus-Implementierung verfügt immer über mindestens eine Site pro physischer Position.

Standardmäßig verfügt die IBM Spectrum Protect Plus-Umgebung über eine primäre Site, eine sekundäre Site und eine Demosite.

Site hinzufügen

Nachdem IBM Spectrum Protect Plus eine Site hinzugefügt wurde, können Sie der Site Sicherungsspeicherserver zuordnen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Site hinzuzufügen:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Site**.
2. Klicken Sie auf **Site hinzufügen**.
   Die Seite **Siteeigenschaften** wird angezeigt.
3. Geben Sie einen Sitenamen ein.
4. Optional: Um die Netzaktivität für einen definierten Zeitplan zu verwalten, ändern Sie den Durchsatz für Sitereplikations- und Auslagerungsoperationen:
   a) Wählen Sie das Kontrollkästchen **Drosselung aktivieren** aus.
   b) Passen Sie im Feld **Rate** den Durchsatz an:
      1) Ändern Sie den numerischen Wert für die Durchsatzrate, indem Sie auf den Aufwärts- oder Abwärtspfeil klicken.
      2) Wählen Sie eine Einheit für den Durchsatz aus. Die Auswahlmöglichkeiten umfassen **Byte/s**, **KB/s**, **MB/s** und **GB/s**.

   Der Standarddurchsatz ist 100 MB/s (Megabyte pro Sekunde).

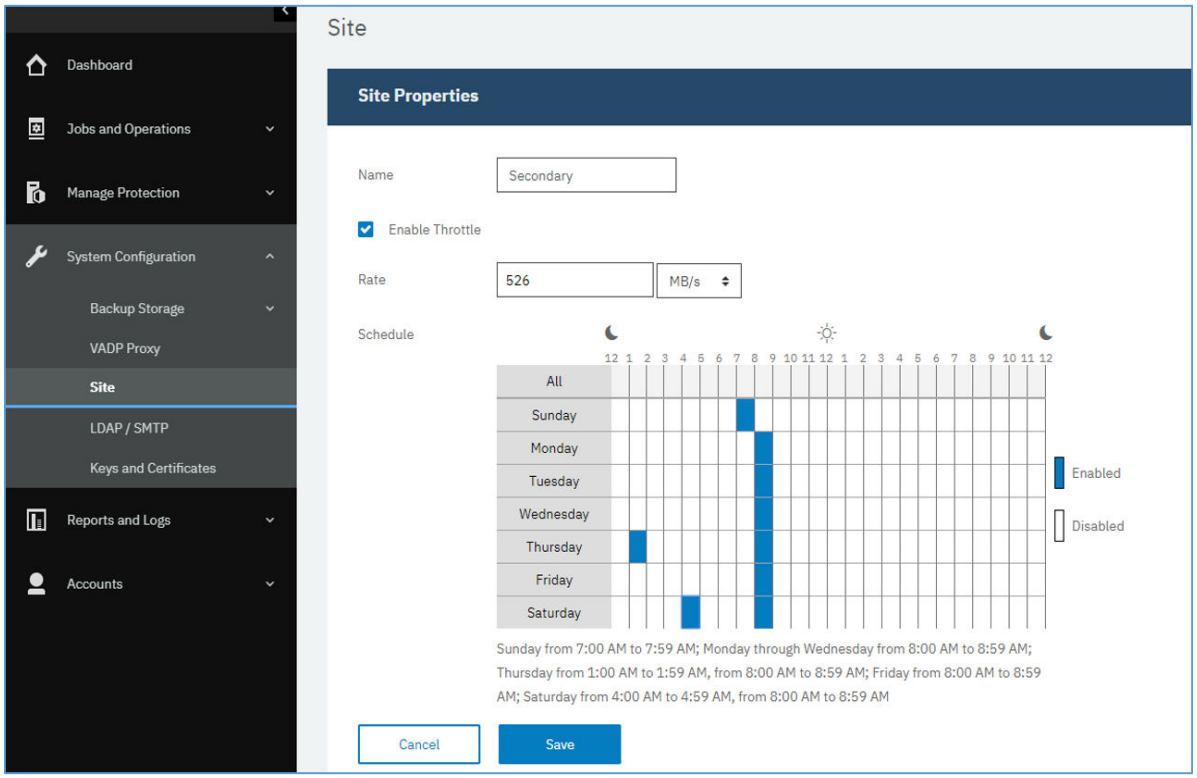


Abbildung 30. Verschiedene Drosselungsraten für verschiedene Zeitpunkte zur Verbesserung des Durchsatzes aktivieren

   c) Wählen Sie in der Tabelle mit dem Wochenplan die Tageszeiten oder bestimmte Tage und Uhrzeiten für die Drosselung aus.

Tipp: Um eine Uhrzeit auszuwählen, klicken Sie in der Tabelle auf ein Zeitintervall. Das ausgewählte Zeitintervall wird hervorgehoben. Um ein Zeitintervall zu löschen, klicken Sie auf das hervorgehobene Zeitintervall. Um dasselbe Zeitintervall für jeden Tag der Woche auszuwählen, klicken Sie in der Zeile **Alle** auf ein Zeitintervall.

Nach der Eingabe Ihrer Auswahlangaben werden die Tage und Uhrzeiten für die Drosselung unter der Tabelle mit dem Zeitplan aufgelistet.

5. Klicken Sie auf **Speichern**, um die Änderungen festzuschreiben und das Fenster zu schließen.

Ergebnisse

Die Site wird in der Tabelle der Sites angezeigt und kann auf neue und vorhandene Sicherungsspeicherserver angewendet werden.

Site editieren

Überarbeiten Sie Siteinformationen, um Änderungen in Ihrer IBM Spectrum Protect Plus-Umgebung widerzuspiegeln.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Site zu editieren:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Site**.
2. Klicken Sie auf das Symbol für Editieren , das einer Site zugeordnet ist.
   Die Seite **Siteeigenschaften** wird angezeigt.
3. Überarbeiten Sie den Sitenamen.
4. Optional: Um die Netzaktivität für einen definierten Zeitplan zu verwalten, ändern Sie den Durchsatz für Sitereplikations- und Auslagerungsoperationen:
   a) Wählen Sie das Kontrollkästchen **Drosselung aktivieren** aus.
   b) Passen Sie im Feld **Rate** den Durchsatz an:
      1) Ändern Sie den numerischen Wert für die Durchsatzrate, indem Sie auf den Aufwärts- oder Abwärtspfeil klicken.
      2) Wählen Sie eine Einheit für den Durchsatz aus. Die Auswahlmöglichkeiten umfassen **Byte/s**, **KB/s**, **MB/s** und **GB/s**.

   Der Standarddurchsatz ist 100 MB/s (Megabyte pro Sekunde).

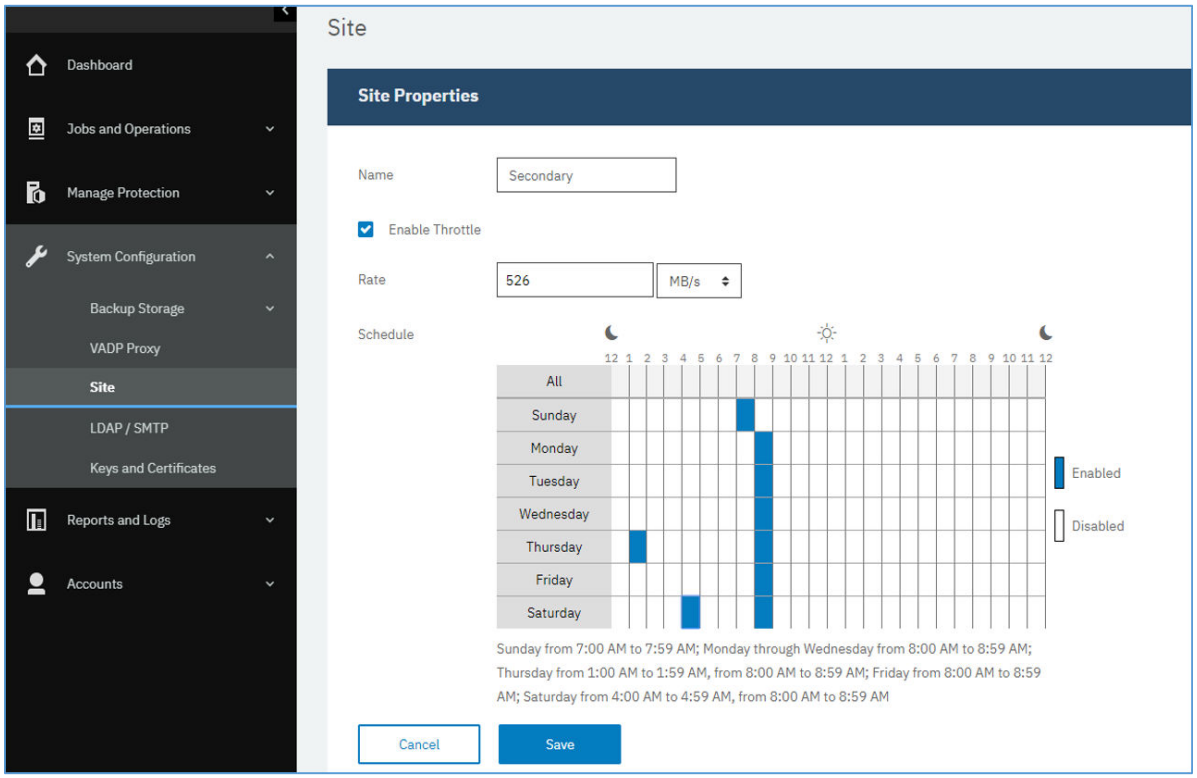


Abbildung 31. Verschiedene Drosselungsraten für verschiedene Zeitpunkte zur Verbesserung des Durchsatzes aktivieren

c) Wählen Sie in der Tabelle mit dem Wochenplan die Tageszeiten oder bestimmte Tage und Uhrzeiten für die Drosselung aus.

Tipp: Um eine Uhrzeit auszuwählen, klicken Sie in der Tabelle auf ein Zeitintervall. Das ausgewählte Zeitintervall wird hervorgehoben. Um ein Zeitintervall zu löschen, klicken Sie auf das hervorgehobene Zeitintervall. Um dasselbe Zeitintervall für jeden Tag der Woche auszuwählen, klicken Sie in der Zeile **Alle** auf ein Zeitintervall.

Nach der Eingabe Ihrer Auswahlangaben werden die Tage und Uhrzeiten für die Drosselung unter der Tabelle mit dem Zeitplan aufgelistet.

5. Klicken Sie auf **Speichern**, um die Änderungen festzuschreiben und das Fenster zu schließen.

Site löschen

Löschen Sie eine Site, wenn sie veraltet ist. Stellen Sie sicher, dass Sie Ihren Sicherungsspeicher anderen Sites neu zuordnen, bevor Sie die Site löschen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Site zu löschen:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Site**.
2. Klicken Sie auf das Symbol für Löschen ✕, das einer Site zugeordnet ist.
3. Klicken Sie auf **Ja**, um die Site zu löschen.

LDAP- und SMTP-Server verwalten

Sie können einen LDAP- (Lightweight Directory Access Protocol) und SMTP-Server (Simple Mail Transfer Protocol) in IBM Spectrum Protect Plus zur Verwendung in Benutzeraccount- und Berichtsfunktionen hinzufügen.

Zugehörige Tasks

„Benutzeraccount für eine LDAP-Gruppe erstellen” auf Seite 320
Fügen Sie IBM Spectrum Protect Plus einen Benutzeraccount für eine LDAP-Gruppe hinzu.

„Bericht planen” auf Seite 309
Sie können die Ausführung angepasster Berichte zu bestimmten Zeiten in IBM Spectrum Protect Plus planen.

LDAP-Server hinzufügen

Sie müssen einen LDAP-Server hinzufügen, um IBM Spectrum Protect Plus-Benutzeraccounts mithilfe einer LDAP-Gruppe zu erstellen. Diese Accounts ermöglichen Benutzern den Zugriff auf IBM Spectrum Protect Plus unter Verwendung von LDAP-Benutzernamen und -Kennwörtern. Einer Instanz der virtuellen IBM Spectrum Protect Plus-Appliance kann nur ein einziger LDAP-Server zugeordnet werden.

Informationen zu diesem Vorgang

Sie können einen Microsoft Active Directory- oder OpenLDAP-Server hinzufügen. Beachten Sie, dass OpenLDAP nicht den Benutzerfilter sAMAaccountName unterstützt, der häufig in Active Directory verwendet wird. Außerdem muss die Option **memberOf** auf dem OpenLDAP-Server aktiviert sein.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen LDAP-Server zu registrieren:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **LDAP/SMTP**.
2. Klicken Sie im Fenster **LDAP-Server** auf **LDAP-Server hinzufügen**.
3. Füllen Sie die folgenden Felder im Fenster **LDAP-Server** aus:

   Hostadresse

   Die IP-Adresse des Hosts oder der logische Name des LDAP-Servers.

   Port

   Der Port, an dem der LDAP-Server empfangsbereit ist. Der Standardport ist 389 für Nicht-SSL-Verbindungen und 636 für SSL-Verbindungen.

   SSL

   Aktivieren Sie die Option SSL, um eine sichere Verbindung zum LDAP-Server herzustellen.

   Vorhandenen Benutzer verwenden

   Aktivieren Sie dieses Feld, um einen zuvor eingegebenen Benutzernamen und ein zuvor eingegebenes Kennwort für den LDAP-Server auszuwählen.

   Bindungsname

   Der definierte Name für Bindung, der für die Authentifizierung der Verbindung zum LDAP-Server verwendet wird. IBM Spectrum Protect Plus unterstützt die einfache Bindung.

   Kennwort

   Das Kennwort, das dem definierten Namen für Bindung zugeordnet ist.

   Basis-DN

   Die Position, an der Benutzer und Gruppen gefunden werden können.

   Benutzerfilter

   Ein Filter, mit dem nur die Benutzer im Basis-DN ausgewählt werden, die bestimmte Kriterien erfüllen. Ein Beispiel für einen gültigen Standardbenutzerfilter ist `cn={0}`.

   Tipps:

   - Um die Authentifizierung mithilfe des Windows-Benutzerbenennungsattributs **sAMAccountName** zu ermöglichen, setzen Sie den Filter auf `samaccountname={0}`. Wenn dieser Filter defi-

niert ist, melden sich Benutzer bei IBM Spectrum Protect Plus an, indem sie nur einen Benutzernamen verwenden. Eine Domäne wird nicht eingeschlossen.

- Um die Authentifizierung mithilfe des UPN-Benennungsattributs (UPN = Benutzerprinzipalname) zu ermöglichen, setzen Sie den Filter auf `userprincipalname={0}`. Wenn dieser Filter definiert ist, melden sich Benutzer bei IBM Spectrum Protect Plus unter Verwendung des Formats Benutzername@Domäne an.
- Um die Authentifizierung mithilfe einer E-Mail-Adresse zu ermöglichen, die LDAP zugeordnet ist, setzen Sie den Filter auf `mail={0}`.

Die Einstellung **Benutzerfilter** steuert außerdem den Typ des Benutzernamens, der in der IBM Spectrum Protect Plus-Anzeige von Benutzern erscheint.

Benutzer-RDN

Der relativ definierte Pfad für den Benutzer. Geben Sie den Pfad an, in dem Benutzerdatensätze gefunden werden können. Ein Beispiel für einen gültigen Standard-RDN ist `cn=Benutzer`.

Gruppen-RDN

Der relativ definierte Pfad für die Gruppe. Wenn sich die Gruppe auf einer anderen Ebene als der Benutzerpfad befindet, geben Sie den Pfad an, in dem Gruppendatensätze gefunden werden können.

4. Klicken Sie auf **Speichern**.

Ergebnisse

IBM Spectrum Protect Plus führt die folgenden Aktionen aus:

1. Es bestätigt, dass eine Netzverbindung hergestellt wird.
2. Es fügt den LDAP-Server der Datenbank hinzu.

Nachdem der SMTP-Server hinzugefügt wurde, ist die Schaltfläche **LDAP-Server hinzufügen** nicht mehr verfügbar.

Nächste Schritte

Wird eine Nachricht zurückgegeben, die angibt, dass die Verbindung nicht erfolgreich ist, überprüfen Sie Ihre Eingaben. Sind Ihre Eingaben korrekt und ist die Verbindung nicht erfolgreich, bitten Sie einen Netzadministrator, die Verbindungen zu überprüfen.

Zugehörige Tasks

„Benutzeraccount für eine LDAP-Gruppe erstellen” auf Seite 320
Fügen Sie IBM Spectrum Protect Plus einen Benutzeraccount für eine LDAP-Gruppe hinzu.

SMTP-Server hinzufügen

Sie müssen einen SMTP-Server hinzufügen, um geplante Berichte an E-Mail-Empfänger senden zu können. Einer virtuellen IBM Spectrum Protect Plus-Appliance kann nur ein einziger SMTP-Server zugeordnet werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen SMTP-Server hinzuzufügen:

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **LDAP/SMTP**.
2. Klicken Sie im Fenster **SMTP-Server** auf **SMTP-Server hinzufügen**.
3. Füllen Sie die folgenden Felder im Fenster **SMTP-Server** aus:

Hostadresse

Die IP-Adresse des Hosts oder der Pfad und der Hostname des SMTP-Servers.

Port

Der Kommunikationsport des Servers, der hinzugefügt wird. Der Standardport ist 25 für Nicht-SSL-Verbindungen und 443 für SSL-Verbindungen.

Benutzername

Der Name, der für den Zugriff auf den SMTP-Server verwendet wird.

Kennwort

Das Kennwort, das dem Benutzernamen zugeordnet ist.

Zeitlimit

Der E-Mail-Zeitlimitwert in Millisekunden.

Ausgangsadresse

Die Adresse, die der E-Mail-Kommunikation von IBM Spectrum Protect Plus zugeordnet ist.

Betreffpräfix

Das Präfix, das den von IBM Spectrum Protect Plus gesendeten E-Mail-Betreffzeilen hinzugefügt werden soll.

4. Klicken Sie auf **Speichern**.

Ergebnisse

IBM Spectrum Protect Plus führt die folgenden Aktionen aus:

1. Es bestätigt, dass eine Netzverbindung hergestellt wird.
2. Es fügt den Server der Datenbank hinzu.

Wird eine Nachricht zurückgegeben, die angibt, dass die Verbindung nicht erfolgreich ist, überprüfen Sie Ihre Eingaben. Sind Ihre Eingaben korrekt und ist die Verbindung nicht erfolgreich, bitten Sie einen Netzadministrator, die Verbindungen zu überprüfen.

Um die SMTP-Verbindung zu testen, klicken Sie auf die Schaltfläche **SMTP-Server testen** und geben Sie dann eine E-Mail-Adresse ein. Klicken Sie auf **Senden**. Eine Test-E-Mail-Nachricht wird an die E-Mail-Adresse gesendet, um die Verbindung zu verifizieren.

Nachdem der SMTP-Server hinzugefügt wurde, ist die Schaltfläche **SMTP-Server hinzufügen** nicht mehr verfügbar.

Nächste Schritte

Zugehörige Tasks

„Bericht planen” auf Seite 309

Sie können die Ausführung angepasster Berichte zu bestimmten Zeiten in IBM Spectrum Protect Plus planen.

Einstellungen für einen LDAP- oder SMTP-Server editieren

Editieren Sie die Einstellungen für einen LDAP- oder SMTP-Server, um Änderungen in Ihrer IBM Spectrum Protect Plus-Umgebung widerzuspiegeln.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Einstellungen für einen LDAP- oder SMTP-Server zu editieren:

1. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **LDAP/SMTP**.
2. Klicken Sie auf das Symbol für Editieren , das dem Server zugeordnet ist.
   Das Editierfenster wird angezeigt.
3. Überarbeiten Sie die Einstellungen für den Server und klicken Sie dann auf **Speichern**.

LDAP- oder SMTP-Server löschen

Löschen Sie einen LDAP- oder SMTP-Server, wenn er veraltet ist. Stellen Sie sicher, dass der Server nicht von IBM Spectrum Protect Plus verwendet wird, bevor Sie den Server löschen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen LDAP- oder SMTP-Server zu löschen:

1. Klicken Sie im Navigationsmenü auf **Systemkonfiguration** > **LDAP/SMTP**.
2. Klicken Sie auf das Symbol für Löschen ✕, das dem Server zugeordnet ist.
3. Klicken Sie auf **Ja**, um den Server zu löschen.

Globale Vorgaben anwenden

Als Administrator können Sie Vorgaben verwalten, die für alle IBM Spectrum Protect Plus-Operationen im Fenster **Globale Vorgaben** gelten.

Vorbereitende Schritte

Globale Vorgaben können nur von dem Benutzer mit Administratorberechtigungsnachweisen verwaltet werden.

Informationen zu diesem Vorgang

Das Fenster **Globale Vorgaben** enthält Standardwerte für Parameter, die für alle IBM Spectrum Protect Plus-Operationen gelten. Die Vorgaben sind in drei Kategorien unterteilt: Anwendung, Schutz und Sicherheit.

Die Standardwerte für die globalen Vorgaben werden in der folgenden Tabelle gezeigt.

Tabelle 23. Standardwerte für globale Vorgaben

Vorgabe	Standardwert	Einheit (sofern zutreffend)
Gleichzeitig ausgeführte Anwendungsserver für Sicherungssitzung	0	
Prozentsatz (%) des freien vSnap-Speicherbereichs - Warnung	30	Prozentsatz (%)
Prozentsatz (%) des freien vSnap-Speicherbereichs - Fehler	20	Prozentsatz (%)
VMs gruppieren nach Größe der VM-Gruppe (GB)	5120	Gigabyte
VMs gruppieren nach Anzahl VMs in Gruppe	20	
VMware-Verbindungszeitlimit	300	Sekunden
Sicherungsaktualisierungsintervall	300	Sekunden
Mindestlänge des Kennworts	8	Zeichen

Sie können die Standardwerte im Fenster **Globale Vorgaben** ändern.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Systemkonfiguration** > **Globale Vorgaben**.
2. Aktualisieren Sie die Werte für die globalen Vorgaben. Um einen zuvor eingegebenen Wert auf den Standardwert zurückzusetzen, klicken Sie auf das Symbol für Zurücksetzen .

Vorgabe	Beschreibung
Anwendung	**Gleichzeitig ausgeführte Anwendungsserver für Sicherungssitzung** Die maximale Anzahl gleichzeitig ausgeführter Anwendungsserver pro Sicherungssitzung.
Sicherung (Hypervisor/Anwendung)	**Prozentsatz (%) des freien vSnap-Speicherbereichs - Warnung** Der Schwellenwert (in Prozent) des verbleibenden freien Speicherbereichs im vSnap-Speicherpool. Im Jobprotokoll werden Warnungen angezeigt. Wenn beispielsweise ein Wert von 10 angegeben wird, wird eine Warnung angezeigt, wenn im vSnap-Speicherpool maximal 10 % freier Speicherbereich verbleiben. **Prozentsatz (%) des freien vSnap-Speicherbereichs - Fehler** Der Schwellenwert (in Prozent) des verbleibenden freien Speicherbereichs im vSnap-Speicherpool. Im Jobprotokoll werden Fehler angezeigt. Wenn beispielsweise ein Wert von 5 angegeben wird, wird ein Fehler angezeigt, wenn im vSnap-Speicherpool maximal 5 % freier Speicherbereich verbleiben.
Hypervisor	**VMs gruppieren** Virtuelle Maschinen können in einer Gruppe zusammengefasst werden. Die Gruppe kann anhand der Anzahl der enthaltenen VMs oder anhand der Größe der in der Gruppe enthaltenen VMs definiert werden. **VMware-Verbindungszeitlimit** Der Zeitraum, den IBM Spectrum Protect Plus auf die Beendigung von Befehlen wartet, die an verbundene vCenter ausgegeben werden. Wenn die Operationen nicht innerhalb des angegebenen Zeitraums beendet werden, werden sie als Fehler protokolliert. Diese Einstellung gilt nur für VMware-Hypervisoren. **Sicherungsaktualisierungsintervall** Die Häufigkeit, mit der Nachrichten zum Fortschritt der Datenübertragung im Jobprotokoll aktualisiert werden.
Sicherheit	**Mindestlänge des Kennworts** Die Mindestlänge von Kennwörtern für IBM Spectrum Protect Plus. Standardmäßig hat das Kennwort eine Mindestlänge von 8 Zeichen; Sie können jedoch ein längeres Kennwort angeben. Dieser Wert gilt für alle Benutzeraccounts.

Anmerkung: Bei einer VM-Gruppierung sind vier VM-Gruppen vorhanden; jede VM-Gruppe kann maximal fünf VMs enthalten. Jede Gruppe entspricht einem einzelnen Zieldatenträger (Datenstrom). Maximal 20 VMs (4 Datenströme) können abhängig von Größenberechnungen gleichzeitig ausgeführt werden.

An der Verwaltungskonsole anmelden

Melden Sie sich an der Verwaltungskonsole an, um die Konfiguration der virtuellen IBM Spectrum Protect Plus-Appliance zu überprüfen. Zu den verfügbaren Informationen gehören allgemeine Systemeinstellungen, Netzeinstellungen und Proxy-Einstellungen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um sich an der Verwaltungskonsole anzumelden:

1. Geben Sie in einem unterstützten Browser die folgende URL ein:

   ```
   https://HOSTNAME:8090/
   ```

   Dabei ist *HOSTNAME* die IP-Adresse der virtuellen Maschine, auf der die Anwendung implementiert ist.
2. Wählen Sie im Anmeldefenster einen der folgenden Authentifizierungstypen in der Liste **Authentifizierungstyp** aus:

Authentifizierungstyp	Anmeldeinformationen
IBM Spectrum Protect Plus	Um sich als IBM Spectrum Protect Plus-Benutzer mit SYSADMIN-Berechtigungen anzumelden, geben Sie Ihren Administratorbenutzernamen und Ihr Kennwort ein.
System	Um sich als Systembenutzer anzumelden, geben Sie die Benutzer-ID `serveradmin` ein. Das Standardkennwort ist `sppDP758`. Sie werden bei der ersten Anmeldung aufgefordert, dieses Kennwort zu ändern.

Nächste Schritte

Überprüfen Sie die Konfiguration der virtuellen IBM Spectrum Protect Plus-Appliance.

Zugehörige Konzepte

„Systemanforderungen” auf Seite 11

Informieren Sie sich vor der Installation von IBM Spectrum Protect Plus über die Hardware- und Softwareanforderungen für die Produktkomponenten und anderen Komponenten, deren Installation in der Speicherumgebung geplant ist.

„Rollen verwalten” auf Seite 315

Rollen definieren die Aktionen, die für die Ressourcen ausgeführt werden können, die in einer Ressourcengruppe definiert sind. Eine Ressourcengruppe definiert die Ressourcen, die einem Account zur Verfügung stehen, und ein Rolle legt die Berechtigungen für die Interaktion mit den Ressourcen fest.

Zeitzone festlegen

Verwenden Sie die Verwaltungskonsole, um die Zeitzone der IBM Spectrum Protect Plus-Appliance festzulegen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Zeitzone festzulegen:

1. Geben Sie in einem unterstützten Browser die folgende URL ein:

   ```
   https://HOSTNAME:8090/
   ```

   Dabei ist *HOSTNAME* die IP-Adresse der virtuellen Maschine, auf der die Anwendung implementiert ist.
2. Wählen Sie im Anmeldefenster einen der folgenden Authentifizierungstypen in der Liste **Authentifizierungstyp** aus:

Authentifizierungstyp	Anmeldeinformationen
IBM Spectrum Protect Plus	Um sich als IBM Spectrum Protect Plus-Benutzer mit SYSADMIN-Berechtigungen anzumelden, geben Sie Ihren Administratorbenutzernamen und Ihr Kennwort ein.

Authentifizierungstyp	Anmeldeinformationen
System	Um sich als Systembenutzer anzumelden, geben Sie die Benutzer-ID `serveradmin` ein. Das Standardkennwort ist `sppDP758`. Sie werden bei der ersten Anmeldung aufgefordert, dieses Kennwort zu ändern.

3. Klicken Sie auf **Systemaktionen ausführen**.
4. Wählen Sie im Abschnitt **Zeitzone ändern** Ihre Zeitzone aus.

   Es wird eine Nachrichten angezeigt, die angibt, dass die Operation erfolgreich ausgeführt wurde. Die ausgewählte Zeitzone wird in allen IBM Spectrum Protect Plus-Protokollen und -Zeitplänen widergespiegelt. Die ausgewählte Zeitzone wird auch in der IBM Spectrum Protect Plus-Appliance angezeigt, wenn der Benutzer mit der Benutzer-ID **serveradmin** angemeldet ist.
5. Um die aktuelle Zeitzone anzuzeigen, wählen Sie auf der Hauptseite der Verwaltungskonsole **Produktinformation** aus.

SSL-Zertifikat über die Verwaltungskonsole hochladen

Um sichere Verbindungen in IBM Spectrum Protect Plus zu erstellen, können Sie ein SSL-Zertifikat, wie beispielsweise ein HTTPS- oder LDAP-Zertifikat, über die Verwaltungskonsole hochladen.

Informationen zu diesem Vorgang

Für HTTPS-Zertifikate werden PEM-codierte Zertifikate mit der Erweiterung `.cer` oder `.crt` unterstützt.

Für LDAP-/Hyper-V-Zertifikate, werden DER-codierte Zertifikate mit der Erweiterung `.cer` oder `.crt` unterstützt. Wenn Sie ein LDAP-SSL-Zertifikat hochladen, müssen Sie sicherstellen, dass IBM Spectrum Protect Plus über Konnektivität zum LDAP-Server verfügt und der LDAP-Server aktiv ist.

Zertifikate im ASCII- und Binärformat werden mit den Standarddateierweiterungen `.pem`, `.cer` und `.crt` akzeptiert. Die Funktion der Verwaltungskonsole zum Importieren von Zertifikaten kann jedoch nicht zum Aktualisieren der Appliance-SSL-Web-Server-Kommunikation verwendet werden. Verwenden Sie zum Hochladen von Zertifikaten im ASCII- und Binärformat die Befehlszeile wie in „SSL-Zertifikat über die Befehlszeile hochladen” auf Seite 294 beschrieben.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um ein SSL-Zertifikat hochzuladen:

1. Fragen Sie Ihren Netzadministrator nach dem Namen des zu exportierenden Zertifikats.
2. Exportieren Sie in einem unterstützten Browser das Zertifikat auf Ihren Computer. Notieren Sie die Position des Zertifikats auf Ihrem Computer. Der Prozess zum Exportieren von Zertifikaten ist abhängig von Ihrem Browser unterschiedlich.
3. Geben Sie in einem unterstützten Browser die folgende URL ein:

   ```
   https://HOSTNAME:8090/
   ```

   Dabei ist *HOSTNAME* die IP-Adresse der virtuellen Maschine, auf der die Anwendung implementiert ist.
4. Wählen Sie im Anmeldefenster einen der folgenden Authentifizierungstypen in der Liste **Authentifizierungstyp** aus:

Authentifizierungstyp	Anmeldeinformationen
IBM Spectrum Protect Plus	Um sich als IBM Spectrum Protect Plus-Benutzer mit SYSADMIN-Berechtigungen anzumelden, geben Sie Ihren Administratorbenutzernamen und Ihr Kennwort ein.

Authentifizierungstyp	Anmeldeinformationen
System	Um sich als Systembenutzer anzumelden, geben Sie die Benutzer-ID `serveradmin` ein. Das Standardkennwort ist sppDP758. Sie werden bei der ersten Anmeldung aufgefordert, dieses Kennwort zu ändern.

5. Klicken Sie auf **Zertifikate verwalten**.
6. Klicken Sie auf **Durchsuchen** und wählen Sie das Zertifikat aus, das hochgeladen werden soll.
7. Klicken Sie auf **SSL-Zertifikat für HTTPS hochladen**.
8. Starten Sie die virtuelle Maschine, auf der die Anwendung implementiert ist, erneut.

SSL-Zertifikat über die Befehlszeile hochladen

Verwenden Sie zum Hochladen von Zertifikaten im ASCII- und Binärformat die Befehlszeile für die virtuelle IBM Spectrum Protect Plus-Appliance. Zertifikate werden mit den Standarddateierweiterungen `.pem`, `.cer` und `.crt` akzeptiert.

Informationen zu diesem Vorgang

Dieser Prozess erfordert, dass Sie den privaten Schlüssel, den öffentlichen Schlüssel und Kettenzertifikate in einer Datei im PKCS12-Format (die häufig als PFX-Datei mit der Erweiterung .p12 bezeichnet wird) packen und diese Datei manuell in den IBM Spectrum Protect Plus-Java-Schlüsselspeicher importieren. Bei der Prozedur wird vorausgesetzt, dass Sie bereits über die privaten und öffentlichen Sicherheitsobjekte sowie alle unterstützenden Sicherheitsobjekte verfügen, die von Ihrem Sicherheitsanbieter in einer Datei im PKCS12-Format mit dem Namen *Name*`.p12` gepackt wurden.

Wenn Sie nicht über diese Datei verfügen, müssen Sie zusammen mit Ihrem Sicherheitsanbieter unter Verwendung eines anderen Servers und/oder OpenSSL die erforderliche Zertifikatssignieranforderung generieren. Packen Sie die empfangenen privaten und öffentlichen Zertifikatsobjekte sowie die Kettenzertifikatsobjekte in die nachfolgend referenzierte erforderliche Datei.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Datei *Name*`.p12` zu importieren:

1. Melden Sie sich mit der Benutzer-ID **serveradmin** bei der virtuellen IBM Spectrum Protect Plus-Appliance an.

   Das Anfangskennwort ist sppDP758.
2. Führen Sie in der Befehlszeile den folgenden Befehl aus:

   ```
   /usr/java/latest/bin/keytool -importkeystore -deststorepass ecx-beta -destkeystore /opt/virgo/configuration/keystore -srckeystore NAME.p12 -srcstoretype PKCS12
   ```
3. Starten Sie die virtuelle Appliance erneut.

An der virtuellen Appliance anmelden

Melden Sie sich mithilfe von vSphere Client an der virtuellen IBM Spectrum Protect Plus-Appliance an, um auf die Befehlszeile zuzugreifen. Sie können auf die Befehlszeile in einer VMware-Umgebung oder in einer Hyper-V-Umgebung zugreifen.

Auf die virtuelle Appliance in VMware zugreifen

Melden Sie sich in einer VMware-Umgebung mithilfe von vSphere Client an der virtuellen IBM Spectrum Protect Plus-Appliance an, um auf die Befehlszeile zuzugreifen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um auf die Befehlszeile der virtuellen Appliance zuzugreifen:

1. Wählen Sie in vSphere Client die virtuelle Maschine aus, auf der IBM Spectrum Protect Plus implementiert ist.
2. Wählen Sie auf der Registerkarte **Zusammenfassung** den Eintrag **Konsole öffnen** aus und klicken Sie in der Konsole.
3. Wählen Sie **Anmelden** aus und geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Der Standardbenutzername ist `serveradmin` und das Standardkennwort ist `sppDP758`.

Nächste Schritte

Geben Sie Befehle ein, um die virtuelle Appliance zu verwalten. Geben Sie `exit` ein, um sich abzumelden.

Auf die virtuelle Appliance in Hyper-V zugreifen

Melden Sie sich in einer Hyper-V-Umgebung mithilfe von vSphere Client an der virtuellen IBM Spectrum Protect Plus-Appliance an, um auf die Befehlszeile zuzugreifen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um auf die Befehlszeile der virtuellen Appliance zuzugreifen:

1. Wählen Sie im Hyper-V-Manager die virtuelle Maschine aus, auf der IBM Spectrum Protect Plus implementiert ist.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Verbinden** aus.
3. Wählen Sie **Anmelden** aus und geben Sie Ihren Benutzernamen und Ihr Kennwort ein. Der Standardbenutzername ist `serveradmin` und das Standardkennwort ist `sppDP758`.

Nächste Schritte

Geben Sie Befehle ein, um die virtuelle Appliance zu verwalten. Geben Sie `exit` ein, um sich abzumelden.

Netzkonnektivität testen

Das IBM Spectrum Protect Plus-Service-Tool testet Hostadressen und -Ports, um festzustellen, ob eine Verbindung hergestellt werden kann. Mit dem Service-Tool können Sie überprüfen, ob zwischen IBM Spectrum Protect Plus und einem Knoten eine Verbindung hergestellt werden kann.

Sie können das Service-Tool über die IBM Spectrum Protect Plus-Befehlszeile oder über Fernzugriff mithilfe einer JAR-Datei ausführen. Wenn eine Verbindung hergestellt werden kann, zeigt das Tool einen grünen Haken an. Wenn keine Verbindung hergestellt werden kann, werden die Fehlerbedingung und mögliche Ursachen und Maßnahmen angezeigt.

Das Tool stellt Anleitungen für die folgenden Fehlerbedingungen bereit:

- Zeitlimitüberschreitung
- Verbindungsverweigerung
- Unbekannter Host
- Keine Route

Service-Tool in einer Befehlszeilenschnittstelle ausführen

Sie können das Service-Tool in der Befehlszeilenschnittstelle der virtuellen IBM Spectrum Protect Plus-Appliance starten und in einem Web-Browser ausführen. Anschließend können Sie mithilfe des Service-Tools die Netzkonnektivität zwischen IBM Spectrum Protect Plus und einem Knoten überprüfen.

Vorgehensweise

1. Melden Sie sich bei der virtuellen IBM Spectrum Protect Plus-Appliance mit der Benutzer-ID `serveradmin` an und greifen Sie auf die Eingabeaufforderung zu. Geben Sie den folgenden Befehl aus:

   ```
   # sudo bash
   ```

2. Öffnen Sie Port 9000 in der Firewall, indem Sie den folgenden Befehl ausgeben:

   ```
   # firewall-cmd –add-port=9000/tcp
   ```

3. Führen Sie das Tool aus, indem Sie den folgenden Befehl ausgeben:

   ```
   # java -Dserver.port=9000 -jar /opt/ECX/spp/public/assets/tool/ngxdd.jar
   ```

4. Um die Verbindung zu dem Tool herzustellen, geben Sie in einem Browser die folgende URL ein:

   ```
   http://Hostname:9000
   ```

   Dabei gibt *Hostname* die IP-Adresse der virtuellen Maschine an, auf der die Anwendung implementiert ist.

5. Um den zu testenden Knoten anzugeben, füllen Sie die folgenden Felder aus:

   Host
   Der Hostname oder die IP-Adresse des Knotens, der getestet werden soll.

   Port
   Der zu testende Verbindungsport.

6. Klicken Sie auf **Speichern**.
7. Um das Tool auszuführen, bewegen Sie den Mauszeiger über das Tool und klicken Sie dann auf die grüne Schaltfläche **Ausführen**.

   Wenn keine Verbindung hergestellt werden kann, wird die Fehlerbedingung zusammen mit möglichen Ursachen und Aktionen angezeigt.

8. Stoppen Sie das Tool, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

   ```
   ctl-c
   ```

9. Schützen Sie Ihre Speicherumgebung, indem Sie die Firewall zurücksetzen. Geben Sie die folgenden Befehle aus:

   ```
   # firewall-cmd --zone=public --remove-port=9000/tcp
   # firewall-cmd --runtime-to-permanent
   # firewall-cmd --reload
   ```

   Anmerkung: Wenn der Befehl `firewall-cmd` auf Ihrem System nicht verfügbar ist, editieren Sie die Firewall manuell, um die erforderlichen Ports hinzuzufügen, und starten Sie die Firewall mithilfe von `iptables` erneut. Weitere Informationen zum Editieren von Firewallregeln enthält der Abschnitt **Firewall configuration using iptables** unter https://www.ibm.com/support/knowledgecenter/en/STXKQY_5.0.3/com.ibm.spectrum.scale.v5r03.doc/bl1adv_firewallportopenexamples.htm.

Service-Tool über Fernzugriff ausführen

Sie können das Service-Tool als .jar-Datei in der IBM Spectrum Protect Plus-Benutzerschnittstelle herunterladen. Anschließend können Sie mithilfe des Service-Tools die Netzkonnektivität zwischen IBM Spectrum Protect Plus und einem Knoten über Fernzugriff testen.

Vorgehensweise

1. Klicken Sie in der IBM Spectrum Protect Plus-Benutzerschnittstelle auf das Benutzermenü und dann auf **Testtool herunterladen**.

   Eine .jar-Datei wird auf Ihre Workstation heruntergeladen.

2. Starten Sie das Tool in einer Befehlszeilenschnittstelle. Java™ ist nur auf dem System erforderlich, auf dem das Tool gestartet wird. Für Endpunkte oder Zielsysteme, die von dem Tool getestet werden, ist Java nicht erforderlich.

   Mit dem folgenden Befehl wird das Tool in einer Linux-Umgebung gestartet:

   ```
   # java -jar -Dserver.port=9000 /<Toolpfad>/ngxdd.jar
   ```

3. Um die Verbindung zu dem Tool herzustellen, geben Sie in einem Browser die folgende URL ein:

   ```
   http://Hostname:9000
   ```

   Dabei gibt *Hostname* die IP-Adresse der virtuellen Maschine an, auf der die Anwendung implementiert ist.

4. Um den zu testenden Knoten anzugeben, füllen Sie die folgenden Felder aus:

   Host
   Der Hostname oder die IP-Adresse des Knotens, der getestet werden soll.

   Port
   Der zu testende Verbindungsport.

5. Klicken Sie auf **Speichern**.
6. Um das Tool auszuführen, bewegen Sie den Mauszeiger über das Tool und klicken Sie dann auf die grüne Schaltfläche **Ausführen**.

   Wenn keine Verbindung hergestellt werden kann, wird die Fehlerbedingung zusammen mit möglichen Ursachen und Aktionen angezeigt.

7. Stoppen Sie das Tool, indem Sie in der Befehlszeile den folgenden Befehl ausgeben:

   ```
   ctl-c
   ```

Virtuelle Platten hinzufügen

Sie können Ihrer virtuellen IBM Spectrum Protect Plus-Appliance mithilfe von vCenter neue virtuelle Platten (Festplatten) hinzufügen.

Wenn Sie die virtuelle IBM Spectrum Protect Plus-Appliance implementieren, können Sie alle virtuellen Platten in einem einzigen Datenspeicher implementieren, den Sie während der Implementierung angeben. Sie können eine Platte innerhalb der virtuellen Appliance hinzufügen und als Logical Volume Manager (LVM) konfigurieren. Dann können Sie die neue Platte als neuen Datenträger bereitstellen oder den vorhandenen Datenträgern innerhalb der virtuellen Appliance zuordnen.

Sie können die Plattenpartitionen mit dem Befehl **`fdisk -l`** überprüfen. Sie können die physischen Datenträger und die Datenträgergruppen in der virtuellen IBM Spectrum Protect Plus-Appliance mit den Befehlen **`pvdisplay`** und **`vgdisplay`** überprüfen.

Platte der virtuellen Appliance hinzufügen

Verwenden Sie den vCenter-Client, um die Einstellungen der virtuellen Maschine zu editieren.

Vorbereitende Schritte

Um Befehle ausführen zu können, müssen Sie mithilfe von Secure Shell (SSH) die Verbindung zur Befehlszeile der virtuellen IBM Spectrum Protect Plus-Appliance herstellen und sich mit der Benutzer-ID `serveradmin` anmelden. Das Standardanfangskennwort ist sppDP758; bei der ersten Anmeldung werden Sie zum Ändern des Kennworts aufgefordert.

Vorgehensweise

Führen Sie im vCenter-Client die folgenden Schritte aus, um einer virtuellen IBM Spectrum Protect Plus-Appliance eine Platte hinzuzufügen:

1. Führen Sie im vCenter-Client die folgenden Schritte aus:
   a) Klicken Sie auf der Registerkarte **Hardware** auf **Hinzufügen**.
   b) Wählen Sie **Neue virtuelle Platte erstellen** aus.
   c) Wählen Sie die erforderliche Plattengröße aus. Wählen Sie im Abschnitt **Position** eine der folgenden Optionen aus:
      - Um den aktuellen Datenspeicher zu verwenden, wählen Sie **Mit der virtuellen Maschine speichern** aus.
      - Um eine oder mehrere Datenspeicher für die virtuelle Platte anzugeben, wählen Sie **Datenspeicher oder Datenspeichercluster angeben** aus. Klicken Sie auf **Durchsuchen**, um die neuen Datenspeicher auszuwählen.
   d) Übernehmen Sie auf der Registerkarte **Erweiterte Optionen** die Standardwerte.
   e) Überprüfen und speichern Sie Ihre Änderungen.
   f) Klicken Sie auf die Option **Einstellungen editieren** für die virtuelle Maschine, um die neue Festplatte anzuzeigen.
2. Fügen Sie die neue SCSI-Einheit hinzu, ohne die virtuelle Einheit neu zu starten. Geben Sie in der Konsole der IBM Spectrum Protect Plus-Appliance den folgenden Befehl aus:

   ```
   echo "-- -" > /sys/class/scsi_host/host#/scan
   ```

   Dabei ist # die letzte Hostnummer.

Speicherkapazität einer neuen Platte dem Appliance-Datenträger hinzufügen

Nachdem Sie der virtuellen Appliance eine Platte hinzugefügt haben, können Sie die neue Platte an die vorhandenen Datenträger in der virtuellen Appliance anhängen.

Vorbereitende Schritte

Um Befehle ausführen zu können, müssen Sie mithilfe von SSH die Verbindung zur Konosole der virtuellen IBM Spectrum Protect Plus-Appliance herstellen und sich mit der Benutzer-ID **serveradmin** anmelden. Das Standardanfangskennwort ist sppDP758; bei der ersten Anmeldung werden Sie zum Ändern des Kennworts aufgefordert.

Informationen zu diesem Vorgang

Sie müssen diese Task nur ausführen, wenn die Speicherkapazität einer neuen Platte einem vorhandenen Appliance-Datenträger hinzugefügt werden soll. Wenn Sie die Platte als neuen Datenträger hinzugefügt hatten, müssen Sie diese Task nicht ausführen.

Vorgehensweise

Führen Sie in der Konsole der virtuellen Appliance die folgenden Schritte aus, um dem Appliance-Datenträger die Speicherkapazität einer neuen Platte hinzuzufügen:

1. Führen Sie die folgenden Schritte aus, um eine Partition für die neue Platte einzurichten und für die Partition "Linux LVM" als Typ festzulegen:
   a) Öffnen Sie die neue Platte mit dem Befehl **`fdisk`**:

      ```
      [serveradmin@localhost ~]# fdisk /dev/sdd
      ```

      Das Dienstprogramm **`fdisk`** wird im interaktiven Modus gestartet. Es wird eine ähnliche Ausgabe wie die folgende angezeigt:

```
Device contains neither a valid DOS partition table, nor Sun, SGI or
OSF disklabel
Building a new DOS disklabel with disk identifier 0xb1b293df.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.
Warning: invalid flag 0x0000 of partition table 4 will be corrected by
w(rite)
WARNING: DOS-compatible mode is deprecated. It's strongly recommended
to
switch off the mode (command 'c') and change display units to
sectors (command 'u').
Command (m for help):
```

a) Geben Sie in der **fdisk**-Befehlszeile den Unterbefehl **n** ein, um eine Partition hinzuzufügen.

```
Command (m for help): n
```

Die folgenden Auswahlmöglichkeiten für die Befehlsaktion werden angezeigt:

```
Command (m for help): n
Command action
e extended
p primary partition (1-4)
```

b) Geben Sie die Befehlsaktion **p** ein, um die primäre Partition auszuwählen.
Sie werden zur Eingabe einer Partitionsnummer aufgefordert:

```
Command (m for help): n
Command action
e extended
p primary partition (1-4)
Partition number (1-4):
```

c) Geben Sie in der Eingabeaufforderung für die Partitionsnummer die Partitionsnummer 1 ein.

```
Partition number (1-4): 1
```

Die folgende Eingabeaufforderung wird angezeigt:

```
First cylinder (1-2610, default 1):
```

d) Nehmen Sie in der Eingabeaufforderung für den ersten Zylinder keine Eingabe vor. Drücken Sie die **Eingabetaste**.
Die folgende Ausgabe und Eingabeaufforderung werden angezeigt:

```
First cylinder (1-2610, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610):
```

e) Nehmen Sie in der Eingabeaufforderung für den letzten Zylinder keine Eingabe vor. Drücken Sie die **Eingabetaste**.
Die folgende Ausgabe wird angezeigt:

```
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610):
Using default value 2610
Command (m for help):
```

f) Geben Sie in der **fdisk**-Befehlszeile den Unterbefehl **t** ein, um die System-ID einer Partition zu ändern.

```
Command (m for help): t
```

Sie werden zur Eingabe eines hexadezimalen Codes aufgefordert, der den Partitionstyp angibt:

```
Selected partition 1
Hex code (type L to list codes):
```

g) Geben Sie in der Eingabeaufforderung für den hexadezimalen Code den hexadezimalen Code 8e ein, um den Partitionstyp "Linux LVM" anzugeben.
Die folgende Ausgabe wird angezeigt:

```
Hex code (type L to list codes): 8e
Changed system type of partition 1 to 8e (Linux LVM)
Command (m for help):
```

h) Geben Sie in der **fdisk**-Befehlszeile den Unterbefehl **w** ein, um die Partitionstabelle zu schreiben und das Dienstprogramm **fdisk** zu verlassen.

```
Command (m for help): w
```

Die folgende Ausgabe wird angezeigt:

```
Command (m for help): w (write table to disk and exit)
The partition table has been altered!
Calling ioctl() to re-read partition table.
Syncing disks.
```

2. Um die Änderungen an der Platte zu überprüfen, geben Sie den Befehl **fdisk -1** aus.
3. Um die aktuelle Liste der physischen Datenträger (PV = Physical Volume) zu überprüfen, geben Sie den Befehl **pvdisplay** aus.
4. Um einen neuen physischen Datenträger (PV) zu erstellen, geben Sie den Befehl **pvcreate /dev/sdd1** aus.
5. Um den neuen physischen Datenträger (PV) in /dev/sdd1 anzuzeigen, geben Sie den Befehl **pvdisplay** aus.
6. Um die Datenträgergruppe (VG = Volume Group) zu überprüfen, geben Sie den Befehl **vgdisplay** aus.
7. Um den physischen Datenträger (PV) der Datenträgergruppe (VG) hinzuzufügen und den Speicherbereich der VG zu vergrößern, geben Sie den folgenden Befehl aus:

```
vgextend data_vg /dev/sdd1
```

8. Um zu überprüfen, ob data_vg erweitert wurde und freier Speicherbereich für logische Datenträger (oder den Datenträger /data) verfügbar ist, geben Sie den Befehl **vgdisplay** aus.
9. Um den logischen Datenträger (LV) /data zu überprüfen, geben Sie den Befehl **lvdisplay** aus. Die Datenträgerbelegung für den Datenträger /data wird angezeigt.
10. Um den Speicherbereich des logischen Datenträgers (LV) /data der Gesamtkapazität des Datenträgers hinzuzufügen, geben Sie den Befehl **lvextend** aus.
In diesem Beispiel werden einem 100-GB-Datenträger 20 GB Speicherbereich hinzugefügt.

```
[serveradmin@localhost ~]# lvextend -L120gb -r /dev/data_vg/data
Size of logical volume data_vg/data changed from 100.00 GiB to 120.00 GiB .
Logical volume data successfully resized
resize2fs 1.41.12 (date)
Filesystem at /dev/mapper/data_vg-data is mounted on /data; on-line
resizing required
old desc_blocks = 7, new_desc_blocks = 8
Performing an on-line resize of /dev/mapper/data_vg-data to 31195136
(4k) blocks.
The filesystem on /dev/mapper/data_vg-data is now 31195136 blocks
long.
```

Im Anschluss an die Ausführung des vorherigen Befehls wird die Größe des Datenträgers /data im Befehl **lvdisplay** mit 120 GB angezeigt:

```
[serveradmin@localhost ~]# lvdisplay
--- Logical volume ---
LV Path: /dev/data_vg/data
LV Name: data
VG Name: data_vg
LV UUID: [uuid]
LV Write Access: read/write
LV Creation host, time localhost.localdomain, [date, time]
LV Status: available
# open: 1
LV Size: 120.00 GiB
Current LE: 30208
Segments : 2
Allocation inherit
Read ahead sectors: auto
- currently set to: 256
Block device: 253:1
[serveradmin@localhost ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sda3 14G 2.6G 11G 20% /
tmpfs 16G 0 16G 0% /dev/shm
/dev/sda1 240M 40M 188M 18% /boot
/dev/mapper/data_vg-data
118G 6.4G 104G 6% /data
/dev/mapper/data2_vg-data2
246G 428M 234G 1% /data2
```

Kapitel 12. Berichte und Protokolle verwalten

IBM Spectrum Protect Plus stellt eine Reihe vordefinierter Berichte bereit, die Sie Ihren Berichtsanforderungen entsprechend anpassen können. Darüber hinaus wird ein Protokoll der Aktionen bereitgestellt, die Benutzer in IBM Spectrum Protect Plus ausführen.

Berichtstypen

Sie können vordefinierte Berichte anpassen, um die Auslastung des Sicherungsspeichers und andere Aspekte Ihrer Systemumgebung zu überwachen.

Berichte basieren auf den Daten, die vom neuesten Bestandsjob erfasst werden. Sie können Berichte nach der Beendigung aller Katalogisierungsjobs und nachfolgender Datenbankkomprimierungsjobs generieren. Sie können folgende Berichtstypen ausführen:

- Sicherungsspeichernutzungsberichte
- Schutzberichte
- Systemberichte
- Berichte für Umgebungen virtueller Maschinen

Die Berichte enthalten interaktive Elemente wie z. B. die Suche nach einzelnen Werten in einem Bericht, vertikales Verschieben und Spaltensortierung.

Sicherungsspeichernutzungsberichte

IBM Spectrum Protect Plus stellt Sicherungsspeichernutzungsberichte bereit, in denen die Speichernutzung und der Status Ihres Sicherungsspeichers, z. B. vSnap-Server, angezeigt wird.

Führen Sie die folgenden Schritte aus, um Sicherungsspeichernutzungsberichte anzuzeigen:

1. Klicken Sie im Navigationsfenster auf **Berichte und Protokolle** > **Berichte**.
2. Blenden Sie **Sicherungsspeichernutzung** im Fenster **Berichte** ein.

Folgende Berichte sind verfügbar:

VM-Sicherungsnutzung
Überprüfen Sie die Nutzung Ihrer VM-Sicherungen im Sicherungsspeicher, einschließlich der folgenden Daten:

- Der Name jeder VM, ihre Position und der zugehörige Hypervisor
- Die SLA-Richtlinie, die zum Schützen der VM verwendet wird
- Die Position des Sicherungsspeichers. Der Sicherungsspeicher kann der Hostname oder die IP-Adresse einer Platte, der Name eines Cloud-Servers oder der Name eines Repository-Servers sein.
- Die Größe der einzelnen VM-Sicherungen
- Die Anzahl Zurückschreibungspunkte, die für jede VM verfügbar sind

Um bei virtuellen VMware-Maschinen Ihre Ergebnisse auf die VMs einzugrenzen, die über VMware-Tags verfügen, wählen Sie im Dropdown-Menü **Tags** einen oder mehrere verfügbare Tags aus. Der Standardwert ist **Alle**; damit werden Daten für alle VM-Sicherungen angezeigt.

Bericht "vSnap-Speichernutzung"
Sie können die Speichernutzung Ihrer vSnap-Server überprüfen, einschließlich des Verfügbarkeitsstatus, des freien Speicherbereichs und des belegten Speicherbereichs. Der Bericht "vSnap-Speichernutzung" enthält sowohl eine Übersicht Ihrer vSnap-Server als auch eine Detailsicht der einzelnen virtuellen Maschinen und Datenbanken, die auf jedem vSnap-Server geschützt werden.

Mit den Berichtsoptionen können Sie nach bestimmten vSnap-Servern filtern, die angezeigt werden sollen. Wählen Sie **Per vSnap-Speicher geschützte Ressourcen anzeigen** aus, um eine Detailsicht

© Copyright IBM Corp. 2017, 2019

der einzelnen virtuellen Maschinen und Datenbanken anzuzeigen, die auf jedem vSnap-Server geschützt werden. In diesem Bereich des Berichts werden die Namen der virtuellen Maschinen, der zugehörige Hypervisor, die Position und das Komprimierungs-/Deduplizierungsverhältnis des vSnap-Servers angezeigt.

Bei den von IBM Spectrum Protect Plus angezeigten Werten für die Speicherkapazität und die Speichernutzung kann es Abweichungen zwischen den im Dashboard angezeigten Werten und den im Bericht "vSnap-Speichernutzung" aufgeführten Werten geben. Im Dashboard werden Live-Informationen angezeigt, im Bericht erscheinen dagegen Daten aus der letzten Bestandsjobausführung. Die Unterschiede sind auch auf unterschiedliche Rundungsalgorithmen zurückzuführen.

Zugehörige Konzepte

„Berichtsaktionen” auf Seite 308
Sie können Berichte in IBM Spectrum Protect Plus ausführen, speichern oder planen.

„Berichtstypen” auf Seite 303
Sie können vordefinierte Berichte anpassen, um die Auslastung des Sicherungsspeichers und andere Aspekte Ihrer Systemumgebung zu überwachen.

Schutzberichte

IBM Spectrum Protect Plus stellt Berichte bereit, die den Schutzstatus Ihrer Ressourcen anzeigen. Sie können die Berichte anzeigen und alle erforderlichen Maßnahmen ergreifen, um so zur Gewährleistung des Schutzes Ihrer Daten durch benutzerdefinierte RPO-Parameter beizutragen (RPO = Recovery Point Objective).

Führen Sie die folgenden Schritte aus, um Schutzberichte anzuzeigen:

1. Klicken Sie im Navigationsfenster auf **Berichte und Protokolle** > **Berichte**.
2. Blenden Sie **Schutz** im Fenster **Berichte** ein.

Folgende Berichte sind verfügbar:

Bericht "Geschützte und ungeschützte VMs"

Führen Sie den Bericht "Geschützte und ungeschützte VMs" aus, um den Schutzstatus Ihrer virtuellen Maschinen anzuzeigen. Der Bericht gibt Auskunft über die Gesamtzahl der virtuellen Maschinen, die zum IBM Spectrum Protect Plus-Bestand hinzugefügt werden, bevor Sicherungsjobs gestartet werden.

Mit den Berichtsoptionen können Sie nach Hypervisortyp filtern und bestimmte Hypervisoren auswählen, die angezeigt werden sollen.

Sollen ungeschützte virtuelle Maschinen im Bericht nicht berücksichtigt werden, wählen Sie **Ungeschützte VMs ausblenden** aus.

Sollen virtuelle Maschinen ausgeschlossen werden, die nicht im sekundären Sicherungsspeicher gesichert sind, wählen Sie **Nur VMs mit ausgelagerten Sicherungen anzeigen** aus.

In der **Zusammenfassungssicht** wird eine Übersicht über den Schutzstatus Ihrer virtuellen Maschinen angezeigt. Hierzu gehören die Anzahl der ungeschützten und geschützten virtuellen Maschinen und die verwaltete Kapazität der geschützten virtuellen Maschinen. Die verwaltete Kapazität ist die verwendete Kapazität einer virtuellen Maschine. In der **Detailsicht** werden weitere Informationen zu den geschützten und ungeschützten virtuellen Maschinen bereitgestellt, einschließlich Namen und Position.

Bericht "Geschützte und ungeschützte Datenbanken"

Führen Sie den Bericht "Geschützte und ungeschützte Datenbanken" aus, um den Schutzstatus Ihrer Datenbanken anzuzeigen. Der Bericht gibt Auskunft über die Gesamtzahl der Datenbanken, die zum IBM Spectrum Protect Plus-Bestand hinzugefügt werden, bevor Sicherungsjobs gestartet werden.

Mit den Berichtsoptionen können Sie nach anzuzeigendem Anwendungstyp, Anwendungsserver und Anwendungsservertyp filtern.

Sollen Datenbanken ausgeschlossen werden, die durch hypervisorbasierte Sicherungsjobs geschützt werden, wählen Sie **Im Rahmen von Hypervisorsicherungen geschützte Datenbanken ausblenden** aus.

Sollen ungeschützte Datenbanken im Bericht nicht berücksichtigt werden, wählen Sie **Ungeschützte Datenbanken ausblenden** aus.

In der **Zusammenfassungssicht** wird eine Übersicht über den Schutzstatus Ihres Anwendungsservers angezeigt. Hierzu gehören die Anzahl der ungeschützten und geschützten Datenbanken und die Front-End-Kapazität der geschützten Datenbanken. Die Front-End-Kapazität ist die verwendete Kapazität einer Datenbank. In der **Detailsicht** werden weitere Informationen zu den geschützten und ungeschützten Datenbanken bereitgestellt, einschließlich Namen und Position.

Bericht "VM-Sicherungsprotokoll"

Führen Sie den Bericht "VM-Sicherungsprotokoll" aus, um das Schutzprotokoll bestimmter virtueller Maschinen zu überprüfen. Damit der Bericht ausgeführt werden kann, muss mindestens eine virtuelle Maschine in der Option **VMs** angegeben werden. Sie können mehrere Namen virtueller Maschinen auswählen.

Mit den Berichtsoptionen können Sie nach fehlgeschlagenen oder erfolgreichen Jobs und nach der Zeit der letzten Sicherung filtern. Der Bericht kann nach bestimmten SLA-Richtlinien (SLA = Service-Level-Agreement) weiter gefiltert werden. Klicken Sie in der **Detailsicht** auf das Plussymbol  neben einem zugehörigen Job, um Jobdetails anzuzeigen, z. B. die Ursache eines Jobfehlers oder die Größe einer erfolgreichen Sicherung.

Bericht "Datenbanksicherungsprotokoll"

Führen Sie den Bericht "Datenbanksicherungsprotokoll" aus, um das Schutzprotokoll bestimmter Datenbanken zu überprüfen. Damit der Bericht ausgeführt werden kann, muss mindestens eine Datenbank in der Option **Datenbanken** angegeben werden. Sie können mehrere Datenbanken auswählen.

Mit den Berichtsoptionen können Sie nach fehlgeschlagenen oder erfolgreichen Jobs und nach der Zeit der letzten Sicherung filtern. Der Bericht kann nach bestimmten SLA-Richtlinien weiter gefiltert werden. Klicken Sie in der **Detailsicht** auf das Plussymbol  neben einem zugehörigen Job, um weitere Jobdetails anzuzeigen, z. B. die Ursache eines Jobfehlers oder die Größe einer erfolgreichen Sicherung.

Bericht "RPO-Konformität von VMs mit SLA-Richtlinien"

Im Bericht "RPO-Konformität von VMs mit SLA-Richtlinien" werden virtuelle Maschinen in Relation zu den in SLA-Richtlinien definierten Zielsetzungen für Wiederherstellungspunkt (RPO = Recovery Point Objectives) angezeigt. Der Bericht enthält folgende Informationen:

- Konforme virtuelle Maschinen
- Nicht konforme virtuelle Maschinen
- Virtuelle Maschinen, in denen die letzte Sicherungsjobsitzung fehlgeschlagen ist

Mit den Berichtsoptionen können Sie nach Hypervisortyp filtern und bestimmte Hypervisoren auswählen, die angezeigt werden sollen. Der Bericht kann nach virtuellen Maschinen, die mit den definierten RPO konform oder nicht konform sind, weiter gefiltert werden.

Bericht "RPO-Konformität von Datenbanken mit SLA-Richtlinien"

Im Bericht "RPO-Konformität von Datenbanken mit SLA-Richtlinien" werden Datenbanken in Relation zu den in SLA-Richtlinien definierten Zielsetzungen für Wiederherstellungspunkt (RPO = Recovery Point Objectives) angezeigt. Der Bericht enthält folgende Informationen:

- Konforme Datenbanken
- Nicht konforme Datenbanken
- Datenbanken, in denen die letzte Sicherungsjobsitzung fehlgeschlagen ist

Mit den Berichtsoptionen können Sie nach Anwendungstyp filtern und bestimmte Anwendungsserver auswählen, die angezeigt werden sollen. Der Bericht kann nach Datenbanken, die mit den definierten RPO konform oder nicht konform sind, oder nach Schutztyp weiter gefiltert werden, einschließlich Daten, die in vSnap oder mithilfe der Replikation gesichert wurden.

Zugehörige Konzepte

„Berichtstypen” auf Seite 303

Sie können vordefinierte Berichte anpassen, um die Auslastung des Sicherungsspeichers und andere Aspekte Ihrer Systemumgebung zu überwachen.

Systemberichte

IBM Spectrum Protect Plus stellt Systemberichte bereit, in denen eine detaillierte Sicht des Status Ihrer Konfiguration angezeigt wird, einschließlich Speichersysteminformationen, Jobs und Jobstatus.

Führen Sie die folgenden Schritte aus, um Systemberichte anzuzeigen:

1. Klicken Sie im Navigationsfenster auf **Berichte und Protokolle** > **Berichte**.
2. Blenden Sie **System** im Fenster **Berichte** ein.

Folgende Berichte sind verfügbar:

Bericht "Konfiguration"
Sie können die Konfiguration der Anwendungsserver, der Hypervisoren und des verfügbaren Sicherungsspeichers überprüfen. Mit den Berichtsoptionen können Sie nach Konfigurationstypen filtern, die angezeigt werden sollen. Im Bericht werden der Name der Ressource, der Ressourcentyp, die zugehörige Site und der SSL-Verbindungsstatus angezeigt.

Bericht "Job"
Sie können die verfügbaren Jobs in Ihrer Konfiguration überprüfen. Führen Sie diesen Bericht aus, um Jobs nach Typ, nach ihrer durchschnittlichen Dauer und nach ihrem Prozentsatz der erfolgreichen Ausführung anzuzeigen. Mit den Berichtsoptionen können Sie nach Jobtypen filtern, die angezeigt werden sollen, und nach Jobs, die während eines Zeitraums erfolgreich ausgeführt wurden. In der **Zusammenfassungssicht** werden Jobs nach Typ aufgelistet, zusammen mit der Anzahl Ausführungen, Beendigungen und Fehler einer Jobsitzung. Bei den als 'Andere' aufgelisteten Jobsitzungen handelt es sich um abgebrochene, teilweise ausgeführte, derzeit aktive, übersprungene oder gestoppte Jobs. Klicken Sie in der **Detailsicht** auf das Plussymbol  neben einem zugehörigen Job, um weitere Jobdetails anzuzeigen, z. B. durch einen Sicherungsjob geschützte virtuelle Maschinen, die durchschnittliche Laufzeit und die nächste geplante Ausführungszeit, wenn der Job geplant ist.

Bericht "Lizenz"
Sie können die Konfiguration Ihrer IBM Spectrum Protect Plus-Umgebung in Relation zu lizenzierten Funktionen überprüfen. Dieser Bericht enthält die folgenden Abschnitte und Felder:

Schutz virtueller Maschinen
Im Feld **Gesamtzahl VMs** wird die Gesamtzahl der virtuellen Maschinen angezeigt, die durch Hypervisorsicherungsjobs geschützt werden, sowie die Anzahl virtueller Maschinen, die Anwendungsdatenbanken hosten, die durch Anwendungssicherungsjobs (keine Hypervisorsicherungsjobs) geschützt werden. Im Feld **Front-End-Kapazität** wird die Belegungsgröße dieser virtuellen Maschinen angezeigt.

Schutz physischer Maschinen
Im Feld **Gesamtzahl physischer Server** wird die Gesamtzahl der physischen Anwendungsserver angezeigt, die Datenbanken hosten, die durch Anwendungssicherungsjobs geschützt werden. Im Feld **Front-End-Kapazität** wird die Belegungsgröße dieser physischen Anwendungsserver angezeigt.

Sicherungsspeichernutzung (vSnap)
Im Feld **Gesamtzahl vSnap-Server** wird die Anzahl der vSnap-Server angezeigt, die in IBM Spectrum Protect Plus als Sicherungsziel konfiguriert sind. Im Feld **Zielkapazität** wird die gesamte verwendete Kapazität der vSnap-Server angezeigt (ohne Replikatzieldatenträger).

Zugehörige Konzepte

„Berichtstypen” auf Seite 303

Sie können vordefinierte Berichte anpassen, um die Auslastung des Sicherungsspeichers und andere Aspekte Ihrer Systemumgebung zu überwachen.

Berichte für VM-Umgebungen

IBM Spectrum Protect Plus stellt Berichte für Umgebungen virtueller Maschinen bereit, in denen die Speichernutzung und der Status Ihrer virtuellen Maschinen und Datenspeicher angezeigt wird.

Führen Sie die folgenden Schritte aus, um Berichte für Umgebungen virtueller Maschinen anzuzeigen:

1. Klicken Sie im Navigationsfenster auf **Berichte und Protokolle** > **Berichte**.
2. Blenden Sie **VM-Umgebung** im Fenster **Berichte** ein.

Folgende Berichte sind verfügbar:

Bericht "VM-Datenspeicher"

Sie können die Speichernutzung Ihrer Datenspeicher überprüfen, einschließlich des freien Gesamtspeicherbereichs, des bereitgestellten Speicherbereichs und der Kapazitäten. Führen Sie diesen Bericht aus, um Ihre Datenspeicher, die Anzahl virtueller Maschinen in den Datenspeichern und den Prozentsatz des verfügbaren Speicherbereichs anzuzeigen. Mit den Berichtsoptionen können Sie nach Hypervisortyp filtern und bestimmte Hypervisoren auswählen, die angezeigt werden sollen. Der **Detailsichtfilter** legt auf der Basis der Speicherbereichsbelegung in Prozent fest, welche Datenspeicher in der **Detailsicht** angezeigt werden sollen. Verwenden Sie den Filter **Nur verwaiste Datenspeicher anzeigen**, um Datenspeicher anzuzeigen, denen keine virtuellen Maschinen zugeordnet sind, oder virtuelle Maschinen, auf die nicht zugegriffen werden kann. Der Grund für den Verwaisungsstatus eines Datenspeichers wird in der **Detailsicht** im Feld **Datenspeicher** angezeigt.

Bericht "VM-LUNs"

Sie können die Speichernutzung der Nummern logischer Einheiten (LUNs) Ihrer virtuellen Maschinen überprüfen. Führen Sie diesen Bericht aus, um Ihre LUNs, zugehörige Datenspeicher, Kapazitäten und Speicheranbieter anzuzeigen. Mit den Berichtsoptionen können Sie nach Hypervisortyp filtern und bestimmte Hypervisoren auswählen, die angezeigt werden sollen. Verwenden Sie den Filter **Nur verwaiste Datenspeicher anzeigen**, um Datenspeicher anzuzeigen, denen keine virtuellen Maschinen zugeordnet sind, oder virtuelle Maschinen, auf die nicht zugegriffen werden kann.

Bericht "Momentaufnahme-Sprawl"

In diesem Bericht werden das Alter, der Name und die Anzahl der Momentaufnahmen angezeigt, die zum Schutz Ihrer Hypervisorressourcen verwendet werden. Mit den Berichtsoptionen können Sie nach Hypervisortyp filtern und bestimmte Hypervisoren auswählen, die angezeigt werden sollen. Verwenden Sie den Filter **Erstellungszeitpunkt der Momentaufnahme**, um Momentaufnahmen aus bestimmten Zeiträumen anzuzeigen.

Bericht "VM-Sprawl"

Sie können den Status Ihrer virtuellen Maschinen überprüfen, einschließlich virtueller Maschinen, die ausgeschaltet, eingeschaltet oder ausgesetzt sind. Führen Sie diesen Bericht aus, um nicht verwendete virtuelle Maschinen, den Zeitpunkt (Datum und Uhrzeit) ihres Ausschaltens sowie VM-Schablonen anzuzeigen. Mit den Berichtsoptionen können Sie nach Hypervisortyp filtern und bestimmte Hypervisoren auswählen, die angezeigt werden sollen. Der Bericht kann nach Einschaltstatus im Zeitverlauf weiter gefiltert werden, einschließlich der Tage seit dem letzten Ausschalten und der Tage seit dem letzten Aussetzen. Im Abschnitt **Schnellsicht** wird ein Kreisdiagramm des belegten Speicherbereichs und des freien Speicherbereichs in Ihren virtuellen Maschinen auf der Basis des Einschaltstatus angezeigt. Verwenden Sie den Filter **Hypervisor**, um virtuelle Maschinen auf allen Hosts oder auf einem bestimmten Host anzuzeigen. Die Informationen in der **Detailsicht** sind nach Einschaltstatus kategorisiert. Für VM-Schablonen wird eine separate Tabelle bereitgestellt.

Bericht "VM-Speicher"

In diesem Bericht können Sie Ihre virtuellen Maschinen und zugehörigen Datenspeicher überprüfen. Sie können zugehörige Datenspeicher und den bereitgestellten Speicherbereich der Datenspeicher anzeigen. Mit den Berichtsoptionen können Sie nach Hypervisortyp filtern und bestimmte Hypervisoren auswählen, die angezeigt werden sollen. In der **Detailsicht** werden zugehörige Datenspeicher und die Speichermenge im Datenspeicher, die für Dateien der virtuellen Platte zugeordnet ist, angezeigt.

Zugehörige Konzepte

„Berichtstypen” auf Seite 303
Sie können vordefinierte Berichte anpassen, um die Auslastung des Sicherungsspeichers und andere Aspekte Ihrer Systemumgebung zu überwachen.

Berichtsaktionen

Sie können Berichte in IBM Spectrum Protect Plus ausführen, speichern oder planen.

Bericht ausführen

Sie können IBM Spectrum Protect Plus-Berichte mit Standardparametern ausführen oder angepasste Berichte mit angepassten Parametern ausführen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Bericht auszuführen:

1. Klicken Sie im Navigationsfenster auf **Berichte und Protokolle** > **Berichte**.
2. Erweitern Sie einen Berichtstyp und wählen Sie einen Bericht aus, der ausgeführt werden soll.
3. Führen Sie den Bericht entweder mit angepassten Parametern oder mit Standardparametern aus:
   - Um den Bericht mit angepassten Parametern auszuführen, legen Sie die Parameter im Abschnitt **Optionen** fest und klicken Sie auf **Ausführen**. Parameter sind für jeden Bericht eindeutig.
   - Um den Bericht mit Standardparametern auszuführen, klicken Sie auf **Ausführen**.

Nächste Schritte

Überprüfen Sie den Bericht im Fenster **Berichte**.

Zugehörige Konzepte

„Berichte und Protokolle verwalten” auf Seite 303
IBM Spectrum Protect Plus stellt eine Reihe vordefinierter Berichte bereit, die Sie Ihren Berichtsanforderungen entsprechend anpassen können. Darüber hinaus wird ein Protokoll der Aktionen bereitgestellt, die Benutzer in IBM Spectrum Protect Plus ausführen.

Angepassten Bericht erstellen

Sie können vordefinierte Berichte mit angepassten Parametern in IBM Spectrum Protect Plus ändern und die angepassten Berichte speichern.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Bericht zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Berichte und Protokolle** > **Berichte**.
2. Wählen Sie einen vordefinierten Bericht aus.
3. Legen Sie Ihre angepassten Parameter fest.
4. Definieren Sie die Ausführung des Bericht unter einer der folgenden Bedingungen:
   - Bedarfsgesteuerte Ausführung
   - Erstellung eines Zeitplans zur Ausführung des Bericht gemäß der Definition durch die Parameter des Zeitplans
5. Speichern Sie den Bericht mit einem angepassten Namen.

Nächste Schritte

Führen Sie den Bericht aus und überprüfen Sie ihn im Fenster **Berichte**.

Zugehörige Konzepte

„Berichte und Protokolle verwalten” auf Seite 303
IBM Spectrum Protect Plus stellt eine Reihe vordefinierter Berichte bereit, die Sie Ihren Berichtsanforderungen entsprechend anpassen können. Darüber hinaus wird ein Protokoll der Aktionen bereitgestellt, die Benutzer in IBM Spectrum Protect Plus ausführen.

Bericht planen

Sie können die Ausführung angepasster Berichte zu bestimmten Zeiten in IBM Spectrum Protect Plus planen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Bericht zu planen:

1. Klicken Sie im Navigationsfenster auf **Berichte und Protokolle** > **Berichte**.
2. Wählen Sie einen Berichtstyp aus.
3. Wählen Sie den Bericht aus, der geplant werden soll.
4. Editieren Sie die Berichtsparameter im Abschnitt **Optionen**.
5. Geben Sie für den Bericht Werte in die Felder **Name** und **Beschreibung** ein.
6. Definieren Sie die Parameter für den Bericht.
7. Klicken Sie im Abschnitt **Bericht planen** auf **Zeitplan definieren**.
8. Definieren Sie einen Auslöser für den Bericht.
9. Geben Sie in das Feld für die E-Mail-Adresse eine Adresse für den Empfang des geplanten Berichts ein und klicken Sie dann auf **Empfänger hinzufügen**.
10. Klicken Sie auf **Speichern**.

Nächste Schritte

Nach der Berichtsausführung kann der Empfänger den Bericht, der als E-Mail gesendet wird, überprüfen.

Zugehörige Konzepte

„Berichte und Protokolle verwalten” auf Seite 303
IBM Spectrum Protect Plus stellt eine Reihe vordefinierter Berichte bereit, die Sie Ihren Berichtsanforderungen entsprechend anpassen können. Darüber hinaus wird ein Protokoll der Aktionen bereitgestellt, die Benutzer in IBM Spectrum Protect Plus ausführen.

Prüfprotokolle für Aktionen erfassen

Sie können Prüfprotokolle erfassen und nach Aktionen suchen, die in IBM Spectrum Protect Plus ausgeführt wurden.

Vorgehensweise

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

1. Klicken Sie im Navigationsfenster auf **Berichte und Protokolle** > **Prüfprotokolle**.
2. Überprüfen Sie ein Protokoll der Aktionen, die in IBM Spectrum Protect Plus ausgeführt wurden. Die Informationen umfassen die Benutzer, von denen die Aktionen ausgeführt wurden, und Beschreibungen der Aktionen.
3. Um nach den Aktionen eines bestimmten Benutzers in IBM Spectrum Protect Plus zu suchen, geben Sie den Benutzernamen in das Benutzersuchfeld ein.
4. Optional: Erweitern Sie den Abschnitt **Filter**, um die angezeigten Protokolle weiter zu filtern. Geben Sie spezifische Aktionsbeschreibungen und einen Datumsbereich, in dem die Aktion ausgeführt wurde, ein.
5. Klicken Sie auf das Suchsymbol  .
6. Um das Prüfprotokoll als `.csv`-Datei herunterzuladen, klicken Sie auf **Herunterladen** und wählen Sie dann eine Position aus, um die Datei zu speichern.

Zugehörige Konzepte

„Benutzeraccounts verwalten” auf Seite 320

Bevor sich ein Benutzer bei IBM Spectrum Protect Plus anmelden und die verfügbaren Funktionen verwenden kann, muss ein Benutzeraccount in IBM Spectrum Protect Plus erstellt werden.

Kapitel 13. Benutzerzugriff verwalten

Sie können mithilfe der rollenbasierten Zugriffssteuerung die Ressourcen und Berechtigungen festlegen, die IBM Spectrum Protect Plus-Benutzeraccounts zur Verfügung stehen.

Sie können IBM Spectrum Protect Plus für einzelne Benutzer anpassen und ihnen Zugriff auf die von ihnen benötigten Funktionen und Ressourcen gewähren.

Sobald Ressourcen in IBM Spectrum Protect Plus verfügbar sind, können Sie zusammen mit IBM Spectrum Protect Plus-Elementen der höheren Ebene (wie beispielsweise ein Hypervisor und einzelne Anzeigen) einer Ressourcengruppe hinzugefügt werden.

Dann werden Rollen zur Definition der Aktionen konfiguriert, die die Benutzer ausführen können, die der Ressourcengruppe zugeordnet sind. Diese Aktionen werden anschließend mindestens einem Benutzeraccount zugeordnet.

Verwenden Sie die folgenden Abschnitte im Fenster **Accounts**, um rollenbasierten Zugriff zu konfigurieren:

Ressourcengruppen
Eine Ressourcengruppe definiert die Ressourcen, die einem Benutzer zur Verfügung stehen. Jede Ressource, die IBM Spectrum Protect Plus hinzugefügt wird, kann zusammen mit einzelnen IBM Spectrum Protect Plus-Funktionen und -Anzeigen in eine Ressourcengruppe aufgenommen werden. Durch Definieren von Ressourcengruppen können Sie die Funktionalität für den Benutzer optimieren. Eine Ressourcengruppe könnte beispielsweise einen einzelnen Hypervisor enthalten und Zugriff ausschließlich auf Sicherungs- und Berichterstellungsfunktionen haben. Wird die Ressourcengruppe einer Rolle und einem Benutzer zugeordnet, kann der Benutzer nur die Anzeigen aufrufen, die mit der Sicherung und Berichterstellung für den zugeordneten Hypervisor zu tun haben.

Rollen
Rollen definieren die Aktionen, die für die Ressourcen ausgeführt werden können, die in einer Ressourcengruppe definiert sind. Eine Ressourcengruppe definiert die Ressourcen, die einem Benutzeraccount zur Verfügung gestellt werden, und ein Rolle legt die Berechtigungen für die Interaktion mit den in der Ressourcengruppe definierten Ressourcen fest. Wird beispielsweise eine Ressourcengruppe erstellt, die Sicherungs- und Zurückschreibungsjobs enthält, legt die Rolle fest, wie ein Benutzer mit den Jobs interagieren kann.

Es können Berechtigungen angegeben werden, die es einem Benutzer gestatten, die in einer Ressourcengruppe definierten Sicherungs- und Zurückschreibungsjobs zu erstellen, anzuzeigen und auszuführen, aber nicht zu löschen. Genauso können Berechtigungen zum Erstellen von Administratoraccounts angegeben werden, die es einem Benutzer gestatten, andere Accounts zu erstellen und zu bearbeiten, Sites und Ressourcen zu konfigurieren und mit allen verfügbaren IBM Spectrum Protect Plus-Funktionen zu interagieren.

Benutzeraccounts
Ein Benutzeraccount verknüpft eine Ressourcengruppe mit einer Rolle. Damit sich ein Benutzer bei IBM Spectrum Protect Plus anmelden und dessen Funktionen verwenden kann, müssen Sie zunächst den Benutzer als einzelnen Benutzer (wird als 'nativer Benutzer' bezeichnet) oder als Mitglied einer importierten Gruppe von LDAP-Benutzern hinzufügen und anschließend dem Benutzeraccount Ressourcengruppen und Rollen zuordnen. Der Account erhält Zugriff auf die in der Ressourcengruppe definierten Ressourcen und Funktionen sowie die Berechtigungen für die Interaktion mit den in der Rolle definierten Ressourcen und Funktionen.

Benutzerressourcengruppen verwalten

Eine Ressourcengruppe definiert die Ressourcen, die einem Benutzer zur Verfügung gestellt werden. Jede Ressource, die IBM Spectrum Protect Plus hinzugefügt wird, kann zusammen mit einzelnen IBM Spectrum Protect Plus-Funktionen und -Anzeigen in eine Ressourcengruppe aufgenommen werden.

© Copyright IBM Corp. 2017, 2019

Ressourcengruppe erstellen

Erstellen Sie eine Ressourcengruppe, um die Ressourcen zu definieren, die für einen Benutzer verfügbar sind.

Vorbereitende Schritte

Sie können nicht mehr als eine Anwendung pro Maschine einer Ressourcengruppe als Anwendungsserver zuordnen. Wenn beispielsweise SQL und Exchange auf derselben Maschine installiert sind und beide in SPP registriert sind, kann nur eine dieser Anwendungen einer bestimmten Ressourcengruppe als Anwendungsserver hinzugefügt werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ressourcengruppe zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Ressourcengruppe**.
2. Klicken Sie auf **Ressourcengruppe erstellen**. Das Fenster **Ressourcengruppe erstellen** wird angezeigt.
3. Geben Sie einen Namen für die Ressourcengruppe ein.
4. Wählen Sie im Menü **Ich möchte eine Ressourcengruppe erstellen** eine der folgenden Optionen aus:

Option	Aktionen
Neu	a. Wählen Sie einen Ressourcentyp im Menü **Ressourcentyp auswählen** aus. b. Wählen Sie Ressourcensubtypen aus und klicken Sie dann auf **Ressourcen hinzufügen**. Die Ressourcen werden der Sicht **Ausgewählte Ressourcen** hinzugefügt.
Aus Schablone	a. Wählen Sie eine Ressourcengruppe aus der Liste **Welche Ressourcengruppe soll als Schablone verwendet werden?** aus. Die Ressourcen aus der ausgewählten Schablone werden der Sicht **Ausgewählte Ressourcen** hinzugefügt. b. Sie können Ressourcen mithilfe der Liste **Ressourcentyp auswählen** und den zugehörigen Listen hinzufügen. Informationen zum Anzeigen verfügbarer Ressourcentypen und ihrer Verwendung finden Sie in „Ressourcentypen” auf Seite 313.

   Wenn Ressourcen aus der Gruppe gelöscht werden sollen, klicken Sie auf das Symbol für Löschen  , das einer Ressource zugeordnet ist, oder klicken Sie auf **Alles löschen**, um alle Ressourcen zu löschen.
5. Wenn das Hinzufügen von Ressourcen abgeschlossen ist, klicken Sie auf **Ressourcengruppe erstellen**.

Ergebnisse

Die Ressourcengruppe wird in der Tabelle der Ressourcengruppen angezeigt und kann neuen und vorhandenen Benutzeraccounts zugeordnet werden.

Nächste Schritte

Führen Sie nach dem Hinzufügen der Ressourcengruppe die folgende Aktion aus:

Aktion	Vorgehensweise
Erstellen Sie Rollen, um die Aktionen zu definieren, die von dem Benutzeraccount, das der Ressourcengruppe zugeordnet ist, ausgeführt werden können. Rollen dienen zum Definieren von Berechtigungen für die Interaktion mit den Ressourcen, die in der Ressourcengruppe definiert sind.	Siehe „Rolle erstellen” auf Seite 317.

Ressourcentypen

Ressourcentypen werden ausgewählt, wenn Ressourcengruppen erstellt werden; sie legen die Ressourcen fest, die für einen Benutzer, der einer Gruppe zugeordnet ist, verfügbar sind.

Die folgenden Ressourcentypen und Subtypen sind verfügbar:

Ressourcentyp	Subtyp	Beschreibung
Accounts	• Rolle • Benutzer • Identität	Dient zur Erteilung des Zugriffs auf Rollen und Benutzer über das Fenster **Accounts**.
Anwendung	• Db2 • Oracle • SQL-Standalone-/-Failover-Cluster • SQL AlwaysOn	Dient zur Erteilung des Zugriffs zum Anzeigen einzelner Anwendungsdatenbanken auf einem Anwendungsserver in IBM Spectrum Protect Plus.
Anwendungsserver	• Db2 • SQL • Oracle	Dient zur Erteilung des Zugriffs auf Anwendungsserver in IBM Spectrum Protect Plus ohne Zugriff auf einzelne Datenbanken.
Hypervisor	• VMware • Hyper-V	Dient zur Erteilung des Zugriffs auf Hypervisorressourcen.
Job	Keiner	Dient zur Erteilung des Zugriffs auf Bestands-, Sicherungs- und Zurückschreibungsjobs. Die Jobressourcengruppe ist für alle Sicherungs- und Zurückschreibungsoperationen, einschließlich der Zuordnung von SLA-Richtlinien zu Ressourcen, obligatorisch.
Bericht	• Sicherungsspeichernutzung • Schutz • System • VE-Umgebung	Dient zur Erteilung des Zugriffs auf Berichtstypen und einzelne Berichte.

Ressourcentyp	Subtyp	Beschreibung
Anzeige	Keiner	Dient zur Erteilung oder Verweigerung des Zugriffs auf Anzeigen in der IBM Spectrum Protect Plus-Schnittstelle. Wenn bestimmte Anzeigen nicht in eine Ressourcengruppe für einen Benutzer eingeschlossen sind, kann der Benutzer, unabhängig von den Berechtigungen, die dem Benutzer erteilt wurden, nicht auf die in der Anzeige bereitgestellte Funktionalität zugreifen.
SLA-Richtlinie	Keiner	Dient zur Erteilung des Zugriffs auf SLA-Richtlinien für Sicherungsoperationen.
System	Identität	Dient zur Erteilung des Zugriffs auf die Berechtigungsnachweise, die für den Zugriff auf Ihre Ressourcen erforderlich sind. Identitätsfunktionalität ist über das Fenster **System** > **Identität** verfügbar.
Systemkonfiguration	Platte	Dient zur Erteilung des Zugriffs auf vSnap-Sicherungsspeicherserver.
Systemkonfiguration	LDAP	Dient zur Erteilung des Zugriffs auf LDAP-Server für die Benutzerregistrierung.
Systemkonfiguration	Protokolle	Dient zur Erteilung des Zugriffs zum Anzeigen und Herunterladen von Prüf- und Systemprotokollen.
Systemkonfiguration	Script	Dient zur Erteilung des Zugriffs auf hochgeladene Vorscripts und Nachscripts.
Systemkonfiguration	Scriptserver	Dient zur Erteilung des Zugriffs auf Scriptserver, auf denen Scripts während eines Sicherungs- oder Zurückschreibungsjobs ausgeführt werden.
Systemkonfiguration	Site	Dient zur Erteilung des Zugriffs auf Sites, die vSnap-Sicherungsspeicherservern zugeordnet sind.
Systemkonfiguration	SMTP	Dient zur Erteilung des Zugriffs auf SMTP-Server für Jobbenachrichtigungen.
Systemkonfiguration	VADP-Proxy	Dient zur Erteilung des Zugriffs auf VADP-Proxy-Server.

Ressourcengruppe editieren

Sie können eine Ressourcengruppe editieren, um die Ressourcen und Funktionen, die der Gruppe zugeordnet sind, zu ändern. Aktualisierte Ressourcengruppeneinstellungen werden wirksam, wenn sich Benutzeraccounts, die der Ressourcengruppe zugeordnet sind, bei IBM Spectrum Protect Plus anmelden.

Vorbereitende Schritte

Beachten Sie die folgenden Hinweise, bevor Sie eine Ressourcengruppe editieren:

- Wenn Sie angemeldet sind, wenn die Berechtigungen oder Zugriffsberechtigungen für Ihren Benutzeraccount geändert werden, müssen Sie sich abmelden und erneut anmelden, damit die aktualisierten Berechtigungen wirksam werden.
- Sie können jede Ressourcengruppe, die nicht als **Kann nicht geändert werden** gekennzeichnet ist, editieren.

Sie können nicht mehr als eine Anwendung pro Maschine einer Ressourcengruppe als Anwendungsserver zuordnen. Wenn beispielsweise SQL und Exchange auf derselben Maschine installiert sind und beide in SPP registriert sind, kann nur eine dieser Anwendungen einer bestimmten Ressourcengruppe als Anwendungsserver hinzugefügt werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ressourcengruppe zu editieren:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Ressourcengruppe**.
2. Wählen Sie eine Ressourcengruppe aus und klicken Sie auf das Symbol für Optionen ••• für die Ressourcengruppe. Klicken Sie auf **Ressourcen ändern**.
3. Überarbeiten Sie den Ressourcengruppennamen und/oder die Ressourcen.
4. Klicken Sie auf **Ressourcengruppe aktualisieren**.

Ressourcengruppe löschen

Sie können jede Ressourcengruppe, die nicht als **Kann nicht geändert werden** gekennzeichnet ist, löschen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Ressourcengruppe zu löschen:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Ressourcengruppe**.
2. Wählen Sie eine Ressourcengruppe aus und klicken Sie auf das Symbol für Optionen ••• für die Ressourcengruppe. Klicken Sie auf **Ressourcengruppe löschen**.
3. Klicken Sie auf **Ja**.

Rollen verwalten

Rollen definieren die Aktionen, die für die Ressourcen ausgeführt werden können, die in einer Ressourcengruppe definiert sind. Eine Ressourcengruppe definiert die Ressourcen, die einem Account zur Verfügung stehen, und ein Rolle legt die Berechtigungen für die Interaktion mit den Ressourcen fest.

Wird beispielsweise eine Ressourcengruppe erstellt, die Sicherungs- und Zurückschreibungsjobs enthält, legt die Rolle fest, wie ein Benutzer mit den Jobs interagieren kann. Es können Berechtigungen angegeben werden, die es einem Benutzer gestatten, die in einer Ressourcengruppe definierten Sicherungs- und Zurückschreibungsjobs zu erstellen, anzuzeigen und auszuführen, aber nicht zu löschen.

Genauso können Berechtigungen zum Erstellen von Administratoraccounts angegeben werden, die es einem Benutzer gestatten, andere Accounts zu erstellen und zu bearbeiten, Sites und Ressourcen zu konfigurieren und mit allen verfügbaren IBM Spectrum Protect Plus-Funktionen zu interagieren.

Die Funktionalität einer Rolle ist von einer ordnungsgemäß konfigurierten Ressourcengruppe abhängig. Bei der Auswahl einer vordefinierten Rolle und bei der Konfiguration einer angepassten Rolle müssen Sie sicherstellen, dass der Zugriff auf erforderliche IBM Spectrum Protect Plus-Operationen, -Anzeigen und -Ressourcen in Einklang mit dem vorgesehenen Einsatz der Rolle steht.

Folgende Benutzeraccountrollen sind verfügbar:

Application Admin
Mit der Rolle "Application Admin" können Benutzer die folgenden Aktionen ausführen:

- Anwendungsdatenbankressourcen registrieren und ändern, die von einem Administrator delegiert werden.
- Anwendungsdatenbanken SLA-Richtlinien zuordnen.
- Sicherungs- und Zurückschreibungsoperationen ausführen.
- Berichte, auf die der Benutzer zugreifen kann, ausführen und planen.

Der Zugriff auf Ressourcen muss von einem Administrator über das Fenster **Accounts** > **Ressourcengruppen** erteilt werden.

Backup Only
Mit der Rolle "Backup Only" können Benutzer die folgenden Aktionen ausführen:

- Sicherungsoperationen ausführen, editieren und überwachen.
- SLA-Richtlinien, auf die der Benutzer Zugriff hat, anzeigen, erstellen und editieren.

Der Zugriff auf Ressourcen, einschließlich bestimmter Sicherungsjobs, muss von einem Administrator über **Accounts** > **Ressourcengruppen** erteilt werden.

Restore Only
Mit der Rolle "Restore Only" können Benutzer die folgenden Aktionen ausführen:

- Zurückschreibungsoperationen ausführen, editieren und überwachen.
- SLA-Richtlinien, auf die der Benutzer Zugriff hat, anzeigen, erstellen und editieren.

Der Zugriff auf Ressourcen, einschließlich bestimmter Zurückschreibungsjobs, muss von einem Administrator über das Fenster **Accounts** > **Ressourcengruppen** erteilt werden.

Self Service
Mit der Rolle "Self Service" können Benutzer vorhandene Sicherungs- und Zurückschreibungsoperationen überwachen, die von einem Administrator delegiert werden.

Der Zugriff auf Ressourcen, einschließlich bestimmter Jobs, muss von einem Administrator über das Fenster **Accounts** > **Ressourcengruppen** erteilt werden.

SYSADMIN
Die Rolle SYSADMIN ist die Administratorrolle. Mit dieser Rolle ist der Zugriff auf alle Ressourcen und Berechtigungen möglich.

Benutzer mit dieser Rolle können Benutzer hinzufügen und die folgenden Aktionen für alle Benutzer außer `admin` ausführen:

- Benutzeraccounts ändern und löschen
- Benutzerkennwörter ändern
- Benutzerrollen zuordnen

Durch Auswahl von **IBM Spectrum Protect Plus** in der Liste **Authentifizierungstyp** im Anmeldefenster der Konsole und Eingabe von Administratorberechtigungsnachweisen kann ein Administrator auch auf die Verwaltungskonsole zugreifen.

In der Verwaltungskonsole kann der Administrator Software-Updates anwenden, die IBM Spectrum Protect Plus-Appliance erneut starten und die Ortszeitzone festlegen.

Weitere Informationen zur Verwendung der Verwaltungskonsole finden Sie in „An der Verwaltungskonsole anmelden” auf Seite 291.

VM Admin
Mit der Rolle "VM Admin" können Benutzer die folgenden Aktionen ausführen:

- Hypervisorressourcen, auf die der Benutzer zugreifen kann, registrieren und ändern.
- Hypervisoren SLA-Richtlinien zuordnen.
- Sicherungs- und Zurückschreibungsoperationen ausführen.
- Berichte, auf die der Benutzer zugreifen kann, ausführen und planen.

Der Zugriff auf Ressourcen muss von einem Administrator über das Fenster **Accounts** > **Ressourcengruppen** erteilt werden.

Rolle erstellen

Erstellen Sie Rollen, um die Aktionen zu definieren, die von dem Benutzer eines Accounts, das einer Ressourcengruppe zugeordnet ist, ausgeführt werden können. Rollen dienen zum Definieren von Berechtigungen für die Interaktion mit den Ressourcen, die in der Ressourcengruppe definiert sind.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Benutzerrolle zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Rolle**.
2. Klicken Sie auf **Rolle erstellen**. Das Fenster **Rolle erstellen** wird angezeigt.
3. Wählen Sie aus der Liste **Ich möchte eine Rolle erstellen** eine der folgenden Optionen aus:

Option	Aktionen
Neu	Wählen Sie Berechtigungen aus, die auf die Rolle angewendet werden sollen. Standardmäßig sind keine Berechtigungen vorausgewählt.
Aus Schablone	a. Wählen Sie eine Rolle aus dem Menü **Welche Rolle soll als Schablone verwendet werden?** aus. Berechtigungen, die der Schablonenrolle zugeordnet sind, sind standardmäßig ausgewählt. b. Wählen Sie weitere Berechtigungen aus, die auf die Rolle angewendet werden sollen, und löschen Sie Berechtigungen, die nicht erforderlich sind. Informationen zum Anzeigen verfügbarer Berechtigungen und ihrer Verwendung finden Sie in „Berechtigungstypen” auf Seite 317.

4. Geben Sie einen Namen für die Rolle ein und klicken Sie dann auf **Rolle erstellen**.

Ergebnisse

Die neue Rolle wird in der Tabelle der Rollen angezeigt und kann auf neue und vorhandene Benutzeraccounts angewendet werden.

Berechtigungstypen

Berechtigungstypen werden ausgewählt, wenn Benutzeraccounts erstellt werden; sie legen die Berechtigungen fest, die für den Benutzer verfügbar sind.

Die folgenden Berechtigungen sind verfügbar:

Name	Berechtigungen	Beschreibung
Anwendung	Anzeigen	Dient zum Anzeigen einzelner Anwendungsdatenbanken auf einem Anwendungsserver in IBM Spectrum Protect Plus.

Name	Berechtigungen	Beschreibung
Anwendungsserver	Registrieren, Anzeigen, Editieren, Registrierung zurücknehmen	Dient zur Interaktion mit Anwendungsservern, wie beispielsweise SQL- oder Oracle-Server, ohne Zugriff auf einzelne Datenbanken.
Zertifikat	Erstellen, Anzeigen, Editieren, Löschen	Dient zur Interaktion mit SSL-Zertifikaten für den Zugriff auf Cloud-Server.
Cloud	Registrieren, Anzeigen, Editieren, Registrierung zurücknehmen	Dient zur Interaktion mit Cloud-Servern, die als Sicherungsspeicher für Auslagerungen definiert sind.
Hypervisor	Registrieren, Anzeigen, Editieren, Registrierung zurücknehmen, Optionen	Dient zur Interaktion mit virtuellen Hypervisor-Maschinen, wie beispielsweise VMware- oder virtuelle Hyper-V-Maschinen.
Identität und Schlüssel	Erstellen, Anzeigen, Editieren, Löschen	Dient zur Interaktion mit den Berechtigungsnachweisen, die für den Zugriff auf Ihre Ressourcen erforderlich sind. Identitätsfunktionalität ist über das Fenster "Accounts > Identitäten" verfügbar.
LDAP	Registrieren, Anzeigen, Editieren, Registrierung zurücknehmen	Dient zur Interaktion mit LDAP-Servern für die Benutzerregistrierung.
Protokoll	Anzeigen	Dient zum Anzeigen von Prüf- und Systemprotokollen.
Job	Erstellen, Anzeigen, Editieren, Ausführen, Löschen	Dient zur Interaktion mit Bestands-, Sicherungs- und Zurückschreibungsjobs. **Anmerkung:** Wenn der Benutzer über die Berechtigung zum **Ausführen** eines Jobs verfügt, kann er auch die Aktionen **Anhalten**, **Freigeben** und **Angepasste Zurückschreibung** für den Job ausführen.
VADP-Proxy	Registrieren, Anzeigen, Editieren, Registrierung zurücknehmen	Dient zur Interaktion mit VADP.
Bericht	Erstellen, Anzeigen, Editieren, Löschen	Dient zur Interaktion mit Berichten.
Ressourcengruppe	Erstellen, Anzeigen, Editieren, Löschen	Dient zur Interaktion mit Ressourcengruppen, die die IBM Spectrum Protect Plus-Ressourcen definieren, die dem Benutzer zur Verfügung gestellt werden.

Name	Berechtigungen	Beschreibung
Rolle	Erstellen, Anzeigen, Editieren, Löschen	Dient zur Interaktion mit Rollen, die die Aktionen definieren, die für die in einer Ressourcengruppe definierten Ressourcen ausgeführt werden können.
Script	Hochladen, Anzeigen, Ersetzen, Löschen	Dient zur Interaktion mit Vorscripts und Nachscripts, die IBM Spectrum Protect Plus hinzugefügt werden und vor oder nach einem Job ausgeführt werden.
Site	Erstellen, Anzeigen, Editieren, Löschen	Dient zur Interaktion mit Sites, die vSnap-Sicherungsspeicherservern zugeordnet sind.
SMTP	Registrieren, Anzeigen, Editieren, Registrierung zurücknehmen	Dient zur Interaktion mit SMTP-Servern für Jobbenachrichtigungen.
Sicherungsspeicher	Registrieren, Anzeigen, Editieren, Registrierung zurücknehmen	Dient zur Interaktion mit vSnap-Sicherungsspeicherservern.
SLA-Richtlinie	Erstellen, Anzeigen, Editieren, Löschen	Dient zur Interaktion mit SLA-Richtlinien, die Benutzern die Erstellung angepasster Schablonen für Sicherungsjobs ermöglichen.
Benutzer	Erstellen, Anzeigen, Editieren, Löschen	Dient zur Interaktion mit Benutzern, die einer Ressourcengruppe eine Rolle zugeordnet haben, und stellt Zugriff auf die IBM Spectrum Protect Plus-Benutzerschnittstelle bereit.

Rolle editieren

Sie können eine Rolle editieren, um die Ressourcen und Berechtigungen, die der Rolle zugeordnet sind, zu ändern. Aktualisierte Rolleneinstellungen werden wirksam, wenn sich Benutzeraccounts, die der Rolle zugeordnet sind, bei IBM Spectrum Protect Plus anmelden.

Vorbereitende Schritte

Beachten Sie die folgenden Hinweise, bevor Sie eine Rolle editieren:

- Wenn Sie angemeldet sind, wenn die Berechtigungen oder Zugriffsberechtigungen für Ihren Benutzeraccount geändert werden, müssen Sie sich abmelden und erneut anmelden, damit die aktualisierten Berechtigungen wirksam werden.
- Sie können jede Rolle, die nicht als **Kann nicht geändert werden** gekennzeichnet ist, editieren.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Benutzerrolle zu editieren:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Rolle**.
2. Wählen Sie eine Rolle aus und klicken Sie auf das Symbol für Optionen ••• für die Rolle. Klicken Sie auf **Rolle ändern**.
3. Überarbeiten Sie den Rollennamen und/oder die Berechtigungen.
4. Klicken Sie auf **Rolle aktualisieren**.

Rolle löschen

Sie können eine Rolle, die nicht als **Kann nicht geändert werden** gekennzeichnet ist, löschen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Rolle zu löschen:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Rolle**.
2. Wählen Sie eine Rolle aus und klicken Sie auf das Symbol für Optionen ••• für die Rolle. Klicken Sie auf **Rolle löschen**.
3. Klicken Sie auf **Ja**.

Benutzeraccounts verwalten

Bevor sich ein Benutzer bei IBM Spectrum Protect Plus anmelden und die verfügbaren Funktionen verwenden kann, muss ein Benutzeraccount in IBM Spectrum Protect Plus erstellt werden.

Benutzeraccount für einen einzelnen Benutzer erstellen

Fügen Sie einen Account für einen einzelnen Benutzer in IBM Spectrum Protect Plus hinzu. Wenn Sie ein Upgrade von einer Version von IBM Spectrum Protect Plus vor Version 10.1.1 durchführen, müssen Berechtigungen, die Benutzern in der Vorgängerversion zugeordnet waren, in IBM Spectrum Protect Plus erneut zugeordnet werden.

Vorbereitende Schritte

Wenn angepasste Rollen und Ressourcengruppen verwendet werden sollen, erstellen Sie diese, bevor Sie einen Benutzer erstellen. Siehe „Ressourcengruppe erstellen” auf Seite 312 und „Rolle erstellen” auf Seite 317.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Account für einen einzelnen Benutzer zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Benutzer**.
2. Klicken Sie auf **Benutzer hinzufügen**. Das Fenster **Benutzer hinzufügen** wird angezeigt.
3. Klicken Sie auf **Typ des Benutzers oder der Gruppe auswählen, der bzw. die hinzugefügt werden soll** > **Einzelner neuer Benutzer**.
4. Geben Sie einen Namen und ein Kennwort für den Benutzer ein.
5. Wählen Sie im Abschnitt **Rolle zuordnen** eine oder mehrere Rollen für den Benutzer aus.
6. Überprüfen Sie im Abschnitt **Berechtigungsgruppen** die Berechtigungen und Ressourcen, die für den Benutzer verfügbar sind, und klicken Sie dann auf **Weiter**.
7. Ordnen Sie im Abschnitt **Benutzer hinzufügen - Ressourcen zuordnen** dem Benutzer eine oder mehrere Ressourcengruppen zu und klicken Sie dann auf **Ressourcen hinzufügen**.

   Die Ressourcengruppen werden dem Abschnitt **Ausgewählte Ressourcen** hinzugefügt.
8. Klicken Sie auf **Benutzer erstellen**.

Ergebnisse

Der Benutzeraccount wird in der Benutzertabelle angezeigt. Wählen Sie einen Benutzer aus der Tabelle aus, um verfügbare Rollen, Berechtigungen und Ressourcengruppen anzuzeigen.

Benutzeraccount für eine LDAP-Gruppe erstellen

Fügen Sie IBM Spectrum Protect Plus einen Benutzeraccount für eine LDAP-Gruppe hinzu.

Vorbereitende Schritte

Überprüfen Sie die folgenden Prozeduren, bevor Sie einen Benutzeraccount für eine LDAP-Gruppe erstellen:

- Registrieren Sie einen LDAP-Provider in IBM Spectrum Protect Plus. Siehe „LDAP-Server hinzufügen" auf Seite 287.
- Wenn angepasste Rollen und Ressourcengruppen verwendet werden sollen, erstellen Sie diese, bevor Sie einen Benutzer erstellen. Siehe „Ressourcengruppe erstellen" auf Seite 312 und „Rolle erstellen" auf Seite 317.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Benutzeraccount für eine LDAP-Gruppe zu erstellen:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Benutzer**.
2. Klicken Sie auf **Benutzer hinzufügen**. Das Fenster **Benutzer hinzufügen** wird angezeigt.
3. Klicken Sie auf **Typ des Benutzers oder der Gruppe auswählen, der bzw. die hinzugefügt werden soll** > **LDAP-Gruppe**.
4. Wählen Sie eine LDAP-Gruppe aus.
5. Wählen Sie im Abschnitt **Rolle zuordnen** eine oder mehrere Rollen für den Benutzer aus.
6. Überprüfen Sie im Abschnitt **Berechtigungsgruppen** die Berechtigungen und Ressourcen, die für den Benutzer verfügbar sind, und klicken Sie dann auf **Weiter**.
7. Ordnen Sie im Abschnitt **Benutzer hinzufügen - Ressourcen zuordnen** dem Benutzer eine oder mehrere Ressourcengruppen zu und klicken Sie dann auf **Ressourcen hinzufügen**.

   Die Ressourcengruppen werden dem Abschnitt **Ausgewählte Ressourcen** hinzugefügt.
8. Klicken Sie auf **Benutzer erstellen**.

Ergebnisse

Der Benutzeraccount wird in der Benutzertabelle angezeigt. Wählen Sie einen Benutzer aus der Tabelle aus, um verfügbare Rollen, Berechtigungen und Ressourcengruppen anzuzeigen.

Benutzeraccount editieren

Sie können den Benutzernamen, das Kennwort, die zugeordneten Ressourcengruppen und die Rollen für einen Benutzeraccount mit Ausnahme der Accounts von Benutzern, die der Rolle SUPERUSER zugeordnet sind, editieren. Wenn ein Benutzer zur Rolle SUPERUSER gehört, können Sie nur das Kennwort für den Benutzer ändern.

Vorbereitende Schritte

Wenn Sie angemeldet sind, wenn die Berechtigungen oder Zugriffsberechtigungen für Ihren Benutzeraccount geändert werden, müssen Sie sich abmelden und erneut anmelden, damit die aktualisierten Berechtigungen wirksam werden.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um die Berechtigungsnachweise eines Benutzeraccounts zu editieren:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Benutzer**.
2. Wählen Sie einen oder mehrere Benutzer aus. Wenn Sie mehrere Benutzer mit unterschiedlichen Rollen auswählen, können Sie nur die Ressourcen, aber nicht die Rollen der Benutzer ändern.
3. Klicken Sie auf das Symbol für Optionen ***, um die verfügbaren Optionen anzuzeigen. Welche Optionen angezeigt werden, ist von dem oder den ausgewählten Benutzern abhängig.

   Einstellungen ändern
   Editieren Sie den Benutzernamen und das Kennwort, zugeordnete Rollen und Ressourcengruppen.

Ressourcen ändern
Editieren Sie die zugeordneten Ressourcengruppen.

4. Ändern Sie die Einstellungen für den Benutzer und klicken Sie dann auf **Benutzer aktualisieren** oder **Ressourcen zuordnen**.

Benutzeraccount löschen

Sie können jeden Benutzeraccount mit Ausnahme der Accounts von Benutzern, die der Rolle SUPERUSER zugeordnet sind, löschen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um einen Benutzeraccount zu löschen:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Benutzer**.
2. Wählen Sie einen Benutzer aus.
3. Klicken Sie auf das Symbol für Optionen ••• und klicken Sie dann auf **Benutzer löschen**.

Identitäten verwalten

Bei einigen Funktionen in IBM Spectrum Protect Plus sind Berechtigungsnachweise für den Zugriff auf Ihre Ressourcen erforderlich. Beispielsweise stellt IBM Spectrum Protect Plus eine Verbindung zu Oracle-Servern als der lokale Betriebssystembenutzer her, der während der Registrierung angegeben wird, um Tasks wie Katalogisierung, Datenschutz und Datenzurückschreibung auszuführen.

Benutzernamen und Kennwörter für Ihre Ressourcen können im Fenster **Identität** hinzugefügt und bearbeitet werden. Wenn Sie dann für eine Funktion in IBM Spectrum Protect Plus Berechtigungsnachweise für den Zugriff auf eine Ressource benötigen, wählen Sie **Vorhandenen Benutzer verwenden** und eine Identität im Dropdown-Menü aus.

Identität hinzufügen

Fügen Sie eine Identität hinzu, um Benutzerberechtigungsnachweise bereitzustellen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Identität hinzuzufügen:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Identität**.
2. Klicken Sie auf **Identität hinzufügen**.
3. Füllen Sie die Felder im Fenster **Identitätseigenschaften** aus:

   Name

   Geben Sie einen aussagekräftigen Namen ein, um die Identität zu identifizieren.

   Benutzername

   Geben Sie den Benutzernamen ein, der einer Ressource, wie beispielsweise einem SQL- oder Oracle-Server, zugeordnet ist.

   Kennwort

   Geben Sie das Kennwort ein, das einer Ressource zugeordnet ist.
4. Klicken Sie auf **Speichern**.

   Die Identität wird in der Identitätentabelle angezeigt und kann ausgewählt werden, wenn eine Funktion verwendet wird, die Berechtigungsnachweise für den Zugriff auf eine Ressource mithilfe der Option **Vorhandenen Benutzer verwenden** erfordert.

Identität editieren

Sie können eine Identität überarbeiten, um den Benutzernamen und das Kennwort für den Zugriff auf eine zugeordnete Ressource zu ändern.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Identität zu editieren:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Identität**.
2. Klicken Sie auf das Symbol für Editieren , das einer Identität zugeordnet ist.
   Das Fenster **Identitätseigenschaften** wird angezeigt.
3. Überarbeiten Sie den Identitätsnamen, den Benutzernamen und das Kennwort.
4. Klicken Sie auf **Speichern**.
   Die überarbeitete Identität wird in der Identitätentabelle angezeigt und kann ausgewählt werden, wenn eine Funktion verwendet wird, die Berechtigungsnachweise für den Zugriff auf eine Ressource mithilfe der Option **Vorhandenen Benutzer verwenden** erfordert.

Identität löschen

Sie können eine Identität löschen, wenn sie veraltet ist. Wenn eine Identität einem registrierter Anwendungsserver zugeordnet ist, muss sie vom Anwendungsserver entfernt werden, bevor sie gelöscht werden kann. Um die Zuordnung aufzuheben, navigieren Sie zur Seite **Sicherung** > **Anwendungsserver verwalten**, die dem Anwendungsservertyp zugeordnet ist, und editieren Sie dann die Einstellungen des Anwendungsservers.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um eine Identität zu löschen:

1. Klicken Sie im Navigationsfenster auf **Accounts** > **Identität**.
2. Klicken Sie auf das Symbol für Löschen , das einer Identität zugeordnet ist.
3. Klicken Sie auf **Ja**, um die Identität zu löschen.

Kapitel 14. Lizenzierung

Die Lizenzprüfung ist in IBM Spectrum Protect Plus standardmäßig aktiviert, um festzustellen, ob die aktuelle Nutzung der Lizenzberechtigungsstufe entspricht und um mögliche Lizenzverstöße zu verhindern.

IBM Spectrum Protect Plus generiert Berechtigungsprüfprotokolle als Dateien mit der Erweiterung `.slmtag` (IBM® Software License Metric Tag). IBM® License Metric Tool (ILMT) wird dann für die Umsetzung der Datei und für die Generierung von Lizenznutzungsberichten verwendet. Die Informationen in diesem Abschnitt sollen Ihnen bei der Interpretation Ihrer `.slmtag`-Dateien helfen.

Software License Metric (SLM) Tags

IBM Spectrum Protect Plus generiert Berechtigungsprüfprotokolle als Dateien mit der Erweiterung `.slmtag` (IBM® Software License Metric Tag). IBM® License Metric Tool (ILMT) wird dann für die Umsetzung der Datei und für die Generierung von Lizenznutzungsberichten verwendet. Die bereitgestellten Informationen sollen Ihnen bei der Interpretation Ihrer `.slmtag`-Dateien helfen.

In den `.slmtag`-Dateien können Informationen bis zu einer maximalen Dateigröße von 1 MB gespeichert werden. Danach wird die Datei archiviert und eine neue Protokolldatei erstellt. Es werden maximal 10 Protokolldateien aufbewahrt.

Upgradevoraussetzungen: Wenn Sie ein Upgrade von einem früheren Release auf IBM Spectrum Protect Plus 10.1.3 durchführen, müssen Sie den Verwaltungsjob zur Generierung der `.slmtag`-Dateien ausführen. Bei nachfolgenden Upgrades müssen Sie den Verwaltungsjob zur Aktualisierung vorhandener `.slmtag`-Dateien ausführen.

Protokollformat

Die `.slmtag`-Dateien werden im XML-Format gespeichert, wobei neue Metrikdatensätze an das Ende der Datei angehängt werden.

Der folgende Abschnitt zeigt eine `.slmtag`-Beispieldatei:

```
<SchemaVersion>2.1.1</SchemaVersion>
<SoftwareIdentity>
   <SoftwareIdentity name>"IBM Spectrum Protect Plus"</Name>
   <InstanceId>/opt/virgo</InstanceId>
</SoftwareIdentity>
<Metric logTime ="2018-11-05T16:05:09+00:00">
   <Type>HYPERVISOR_SERVER_COUNT</Type>
   <SubType>HYPERVISOR_SERVER_COUNT</SubType>
   <Value>0</Value>
   <Period>
    <StartTime>2018-11-05T16:05:09+00:00</StartTime>
    <EndTime>2018-11-05T16:05:09+00:00</EndTime>
   </Period>
</Metric>
<Metric logTime="2018-11-05T16:05:09+00:00">
   <Type>APPLICATION_INSTANCE_COUNT</Type>
   <SubType>APPLICATION_INSTANCE_COUNT</SubType>
   <Value>0</Value>
   <Period>
    <StartTime>2018-11-05T16:05:09+00:00</StartTime>
    <EndTime>2018-11-05T16:05:09+00:00</EndTime>
   </Period>
</Metric>
```

Im Element `Value` wird hierbei die Anzahl der Hosts in allen Ressourcengruppen angezeigt, in denen Pakete für eine Instanzgruppe zu der im Element `EndTime` angegebenen Zeit implementiert sind.

Die Datei wird im Laufe der Zeit größer und kann bearbeitet werden, um ältere Metrikelemente zu entfernen. Sie müssen die Elemente so lange aufbewahren, dass sie von ILMT überprüft werden können. Die

© Copyright IBM Corp. 2017, 2019

Häufigkeit der Prüfung wird vom ILMT-Administrator festgelegt, normalerweise sollte eine Aufbewahrungsdauer von einem Monat für Elemente jedoch ausreichen.

Protokollposition

Die `.slmtag`-Datei befindet sich im Verzeichnis /data/slmtag.

Zugehörige Konzepte

„Jobtypen" auf Seite 263
Jobs werden zur Ausführung von Sicherungs-, Zurückschreibungs-, Verwaltungs- und Bestandsoperationen in IBM Spectrum Protect Plus verwendet.

Zugehörige Tasks

„Jobs starten" auf Seite 264
Sie können einen Job selbst dann bedarfsgesteuert ausführen, wenn die Ausführung des Jobs gemäß einem Zeitplan festgelegt ist.

Integration in IBM License Metric Tool (ILMT)

IBM License Metric Tool (ILMT) kann Ihnen dabei helfen festzustellen, ob Ihre Systemumgebung den Lizenzierungsanforderungen entspricht.

ILMT stellt nützliche Funktionen zur Verwaltung virtualisierter Umgebungen und zur Messung der Lizenznutzung bereit. ILMT erkennt die in Ihrer Infrastruktur installierte Software, hilft Ihnen bei der Analyse der Nutzungsdaten und ermöglicht die Generierung von Prüfberichten. Jeder Bericht liefert Ihnen unterschiedliche Informationen zu Ihrer Infrastruktur, z. B. die Computergruppen, die Softwareinstallationen und der Inhalt Ihres Softwarekatalogs.

Jeder ILMT-Prüfbericht enthält standardmäßig Daten der zurückliegenden 90 Tage. Sie können die Art und den Umfang der in einem Bericht angezeigten Informationen mit Filtern anpassen und Ihre persönlichen Einstellungen für weitere Verwendungen speichern. Darüber hinaus können Sie die Berichte im CSV- oder PDF-Format exportieren und Berichts-E-Mails planen, damit bestimmte Empfänger benachrichtigt werden, wenn wichtige Ereignisse auftreten.

Weitere Informationen finden Sie in der Produktdokumentation für IBM License Metric Tool.

Kapitel 15. Fehlerbehebung

Für die Diagnose und Lösung von Problemen stehen Fehlerbehebungsprozeduren zur Verfügung.

Eine Liste der bekannten Probleme und Einschränkungen für jedes IBM Spectrum Protect Plus-Release finden Sie unter Technote 2014120.

Protokolldateien für die Fehlerbehebung erfassen

Um Fehler in der IBM Spectrum Protect Plus-Anwendung zu beheben, können Sie ein Archiv der Protokolldateien, die von IBM Spectrum Protect Plus generiert werden, herunterladen.

Vorgehensweise

Führen Sie die folgenden Schritte aus, um Protokolldateien für die Fehlerbehebung zu sammeln:

1. Klicken Sie auf das Benutzermenü und dann auf **Systemprotokolle herunterladen**.

   Die Ausführung des Downloadprozesses kann einige Zeit dauern.
2. Öffnen Sie die ZIP-Datei mit den Protokollen, die einzelne Protokolldateien für unterschiedliche IBM Spectrum Protect Plus-Komponenten enthält.

   Informationen zu Protokolldateien enthalten die Abschnitte zum Sichern unter "Anwendungen schützen" und "Hypervisoren schützen".

Nächste Schritte

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

1. Analysieren Sie die Protokolldateien und führen Sie die geeigneten Aktionen aus, um das Problem zu lösen.
2. Wenn Sie das Problem nicht lösen können und Unterstützung benötigen, übergeben Sie die Protokolldateien an den IBM Software Support.

© Copyright IBM Corp. 2017, 2019

Kapitel 16. Produktnachrichten

IBM Spectrum Protect Plus-Komponenten senden Nachrichten, anhand deren Präfix Sie die Komponente, von der sie stammen, identifizieren können. Suchen Sie mithilfe der Suchoption nach einer bestimmten Nachricht, indem Sie deren eindeutige ID verwenden.

Nachrichten bestehen aus den folgenden Elementen:

- einem aus fünf Buchstaben bestehenden Präfix,
- einer Nummer zur Identifikation der Nachricht,
- Nachrichtentext, der auf dem Bildschirm angezeigt und in Nachrichtenprotokolle geschrieben wird.

Tipp: Suchen Sie mithilfe der Suchfunktion Ihres Browsers unter Verwendung von Strg+F nach dem gewünschten Nachrichtencode.

Das folgende Beispiel enthält das Präfix für den Db2-Agenten. Wenn Sie auf Mehr klicken, werden weitere Details angezeigt, die die Ursache für die Nachricht angeben.

```
Warnung
16. April 2019
9:14:37
GTGGH0098
[myserver1.myplace.irl.ibm.com]
Datenbank AC7 wird nicht gesichert, da sie für die Sicherungsoperation nicht
auswählbar ist.
Mehr
```

IBM Spectrum Protect Plus-Nachrichtenpräfixe

Nachrichten sind unterschiedliche Präfixe zugeordnet, um die Identifikation der Komponente zu erleichtern, von der die Nachricht ausgegeben wird.

In der folgenden Tabelle ist das Präfix angegeben, das der jeweiligen Komponente zugeordnet ist.

Tabelle 24. Nachrichtenpräfixe nach Komponente

Präfix	**Komponente**
CTGGA	IBM Spectrum Protect Plus
CTGGB	IBM Spectrum Protect Plus-vSnap-Server
CTGGC	IBM Spectrum Protect Plus VDAP (VMware und Hyper-V)
CTGGD	IBM Spectrum Protect Plus-Cloud und -S3
CTGGE	IBM Spectrum Protect Plus for Microsoft SQL Server
CTGGF	IBM Spectrum Protect Plus for Oracle
CTGGG	IBM Spectrum Protect Plus for Microsoft Exchange Server
CTGGH	IBM Spectrum Protect Plus for IBM Db2
CTGGI	IBM Spectrum Protect Plus for MongoDB

Eine Liste aller Nachrichten finden Sie im IBM Knowledge Center an dieser Stelle.

© Copyright IBM Corp. 2017, 2019

Anhang A. Suchrichtlinien

Verwenden Sie Filter für die Suche nach einer Datei oder einem Zurückschreibungspunkt.

Sie können eine Zeichenfolge eingeben, um Objekte mit einem Namen zu finden, der exakt mit der Zeichenfolge übereinstimmt. Beispielsweise gibt die Suche nach dem Begriff `string.txt` die exakte Übereinstimmung `string.txt` zurück.

Sucheinträge mit regulären Ausdrücken werden ebenfalls unterstützt. Weitere Informationen finden Sie in Suchen von Text mit regulären Ausdrücken.

Sie können auch die folgenden Sonderzeichen in die Suche einschließen. Vor jedem Sonderzeichen müssen Sie einen umgekehrten Schrägstrich (\) als Escapezeichen verwenden.

```
+ - & | ! ( ) { } [ ] ^ " ~ * ? : \
```

Um beispielsweise nach der Datei `string[2].txt` zu suchen, geben Sie `string\[2\].txt` ein.

Suche mit Platzhalterzeichen

Sie können Platzhalterzeichen am Anfang, in der Mitte oder am Ende einer Zeichenfolge angeben und diese innerhalb einer Zeichenfolge kombinieren.

Suche nach einer übereinstimmenden Zeichenfolge mithilfe eines Sterns

Die folgenden Beispiele zeigen Suchtext mit einem Stern:

- Mit `string*` wird nach Begriffen wie "string", "strings" oder "stringency" gesucht.
- Mit `str*ing` wird nach Begriffen wie "string", "straying" oder "straightening" gesucht.
- Mit `*string` wird nach Begriffen wie "string" oder "shoestring" gesucht.

Sie können mehrere Sterne als Platzhalterzeichen in einer einzigen Textzeichenfolge verwenden; die Verwendung mehrerer Platzhalterzeichen kann eine umfangreiche Suche jedoch beträchtlich verlangsamen.

Suche nach einem einzelnen übereinstimmenden Zeichen mithilfe eines Fragezeichens

Die folgenden Beispiele zeigen Suchtext mit einem Fragezeichen:

- Mit `string?` wird nach Begriffen wie "strings", "stringy" oder "string1" gesucht.
- Mit `st??ring` wird nach Begriffen wie "starring" oder "steering" gesucht.
- Mit `???string` wird nach Begriffen wie "hamstring" oder "bowstring" gesucht.

© Copyright IBM Corp. 2017, 2019

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:

© Copyright IBM Corp. 2017, 2019

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

© Copyright IBM Corp. 2017, 2019

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 verwendeten Leistungsdaten werden als unter bestimmten Betriebsbedingungen abgeleitet dargestellt. 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 Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und 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 Corporation abgeleitet. © Copyright IBM Corp. _Jahr/Jahre angeben_.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der 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 ihrer Tochtergesellschaften in den USA oder anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft, Windows und Windows NT sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

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 von VMware, Inc. oder ihrer Tochtergesellschaften in den USA und/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 nicht weitergeben, anzeigen oder abgeleitete Werke davon erstellen.

Kommerzielle Nutzung
Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Rechte
Abgesehen von den hier gewährten Berechtigungen werden keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum gewährt.

IBM behält sich das Recht vor, die hierin gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und 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 es die für dieses Softwareangebot bereitgestellten Konfigurationen Ihnen als Kunde ermöglichen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen

Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in den Schwerpunkten der IBM Online-Datenschutzerklärung unter http://www.ibm.com/privacy, in der IBM Online-Datenschutzerklärung unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien und auf der Seite "IBM Software Products and Software-as-a-Service Privacy Statement" unter http://www.ibm.com/software/info/product-privacy.

Glossar

Ein Glossar mit Begriffen und Definitionen für die IBM Spectrum Protect-Produktfamilie ist verfügbar.

Siehe das Glossar für IBM Spectrum Protect.

© Copyright IBM Corp. 2017, 2019

Index

I

J

K

L

M

N

O

P

R

S

T

V

W

Z

Gedruckt in den U.S.A.