Sichern von IBM Db2-Ressourcen

SnapCenter software

NetApp
November 06, 2025

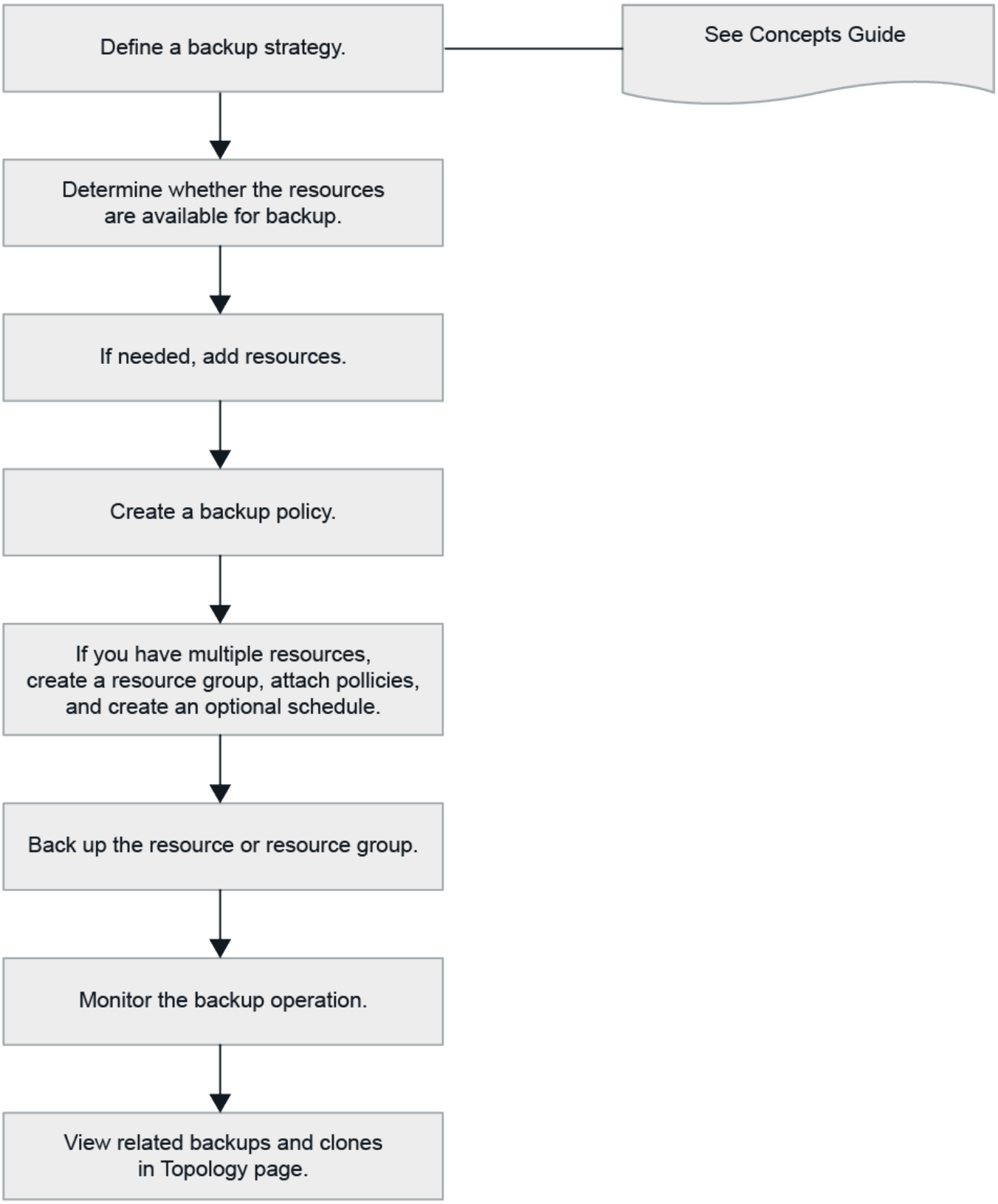
Inhalt

Sichern von IBM Db2-Ressourcen

Sichern von IBM Db2-Ressourcen

Sie können entweder eine Sicherung einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Der Sicherungsworkflow umfasst die Planung, die Identifizierung der zu sichernden Datenbanken, die Verwaltung von Sicherungsrichtlinien, das Erstellen von Ressourcengruppen und Anhängen von Richtlinien, das Erstellen von Sicherungen und die Überwachung der Vorgänge.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie den Sicherungsvorgang durchführen müssen:



Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter -Cmdlet-Hilfe und die Cmdlet-Referenzinformationen enthalten weitere Informationen zu PowerShell-Cmdlets. "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Automatisches Erkennen der Datenbanken

Ressourcen sind IBM Db2-Datenbanken auf dem Linux-Host, die von SnapCenter verwaltet werden. Sie können die Ressourcen zu Ressourcengruppen hinzufügen, um Datenschutzvorgänge durchzuführen, nachdem Sie die verfügbaren IBM Db2-Datenbanken ermittelt haben.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts und das Einrichten der Speichersystemverbindungen abgeschlossen haben.
- Das SnapCenter Plug-in für IBM Db2 unterstützt keine automatische Erkennung der in virtuellen RDM/VMDK-Umgebungen vorhandenen Ressourcen. Sie müssen die Speicherinformationen für virtuelle Umgebungen angeben, während Sie die Datenbanken manuell hinzufügen.

Informationen zu diesem Vorgang

- Nach der Installation des Plug-ins werden alle Datenbanken auf diesem Linux-Host automatisch erkannt und auf der Seite „Ressourcen“ angezeigt.
- Nur Datenbanken werden automatisch erkannt.

Die automatisch erkannten Ressourcen können nicht geändert oder gelöscht werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Plug-in für IBM Db2 aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ den Ressourcentyp aus der Liste „Anzeigen“ aus.
3. (Optional) Klicken Sie auf * * und wählen Sie dann den Hostnamen aus.

   Sie können dann auf * klicken. *, um den Filterbereich zu schließen.
4. Klicken Sie auf **Ressourcen aktualisieren**, um die auf dem Host verfügbaren Ressourcen anzuzeigen.

   Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugehörigen Ressourcengruppen, Sicherungstyp, Richtlinien und Gesamtstatus angezeigt.

   - Wenn sich die Datenbank auf einem NetApp -Speicher befindet und nicht geschützt ist, wird in der Spalte „Gesamtstatus“ „Nicht geschützt“ angezeigt.
   - Wenn sich die Datenbank auf einem NetApp -Speichersystem befindet und geschützt ist und kein Sicherungsvorgang ausgeführt wird, wird in der Spalte „Gesamtstatus“ die Meldung „Sicherung nicht ausgeführt“ angezeigt. Andernfalls ändert sich der Status basierend auf dem letzten Sicherungsstatus in „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“.

Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

Ressourcen manuell zum Plug-In-Host hinzufügen

Die automatische Erkennung wird auf Windows-Hosts nicht unterstützt. Sie müssen Db2-Instanzen und Datenbankressourcen manuell hinzufügen.

Bevor Sie beginnen

- Sie müssen Aufgaben wie die Installation des SnapCenter -Servers, das Hinzufügen von Hosts und das Einrichten von Speichersystemverbindungen abgeschlossen haben.

Informationen zu diesem Vorgang

Die manuelle Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und dann das SnapCenter Plug-in für IBM Db2 aus der Dropdown-Liste aus.
2. Klicken Sie auf der Seite „Ressourcen“ auf **IBM DB2-Ressource hinzufügen**.
3. Führen Sie auf der Seite „Ressourcendetails angeben“ die folgenden Aktionen aus:

Für dieses Feld…	Machen Sie Folgendes…
Name	Geben Sie den Datenbanknamen an.
Hostname	Geben Sie den Hostnamen ein.
Typ	Wählen Sie eine Datenbank oder Instanz aus.
Beispiel	Geben Sie den Namen der Instanz an, die der Datenbank übergeordnet ist.
Anmeldeinformationen	Wählen Sie die Anmeldeinformationen aus oder fügen Sie Informationen zu den Anmeldeinformationen hinzu. Dies ist optional.

4. Wählen Sie auf der Seite „Speicherbedarf angeben“ einen Speichertyp und ein oder mehrere Volumes, LUNs und Qtrees aus und klicken Sie dann auf **Speichern**.

   Optional: Sie können auf das * klicken + * Symbol zum Hinzufügen weiterer Volumes, LUNs und Qtrees aus anderen Speichersystemen.

5. Optional: Geben Sie auf der Seite „Ressourceneinstellungen“ für Ressourcen auf dem Windows-Host benutzerdefinierte Schlüssel-Wert-Paare für das IBM Db2-Plug-In ein.
6. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

   Die Datenbanken werden zusammen mit Informationen wie dem Hostnamen, den zugehörigen Ressourcengruppen und Richtlinien sowie dem Gesamtstatus angezeigt.

Wenn Sie Benutzern Zugriff auf Ressourcen gewähren möchten, müssen Sie die Ressourcen den Benutzern zuweisen. Dadurch können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen zugewiesenen Assets verfügen.

"Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu"

Nachdem Sie die Datenbanken hinzugefügt haben, können Sie die Details der IBM Db2-Datenbank ändern.

Erstellen von Sicherungsrichtlinien für IBM Db2

Bevor Sie SnapCenter zum Sichern von IBM Db2-Ressourcen verwenden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten, planen und aufbewahren.

Bevor Sie beginnen

- Sie müssen Ihre Sicherungsstrategie definiert haben.

  Einzelheiten finden Sie in den Informationen zum Definieren einer Datenschutzstrategie für IBM Db2-Datenbanken.

- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Speichersystemverbindungen und das Hinzufügen von Ressourcen abgeschlossen haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss Ihnen der SnapCenter Administrator die SVMs für das Quell- und das Zielvolume zugewiesen haben.

  Darüber hinaus können Sie in der Richtlinie Replikations-, Skript- und Anwendungseinstellungen angeben. Diese Optionen sparen Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

Informationen zu diesem Vorgang

- SnapLock
  - Wenn die Option „Sicherungskopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock -Aufbewahrungsdauer kleiner oder gleich der angegebenen Aufbewahrungsdauer in Tagen sein.
  - Durch die Angabe einer Snapshot-Sperrfrist wird das Löschen der Snapshots verhindert, bis die Aufbewahrungsfrist abgelaufen ist. Dies kann dazu führen, dass mehr Snapshots aufbewahrt werden als in der Richtlinie angegeben.
  - Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
5. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
   a. Wählen Sie den Speichertyp aus.
   b. Geben Sie im Abschnitt **Benutzerdefinierte Sicherungseinstellungen** alle spezifischen Sicherungseinstellungen an, die im Schlüssel-Wert-Format an das Plug-In übergeben werden müssen.

Sie können mehrere Schlüsselwerte angeben, die an das Plug-In übergeben werden sollen.

6. Führen Sie auf der Seite „Snapshot und Replikation“ die folgenden Aktionen aus.

   a. Geben Sie die Zeitplanhäufigkeit an, indem Sie **Auf Anfrage**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** auswählen.

   Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Sicherungsvorgang beim Erstellen einer Ressourcengruppe angeben. Auf diese Weise können Sie Ressourcengruppen erstellen, die dieselbe Richtlinie und Sicherungshäufigkeit verwenden, aber auch jeder Richtlinie unterschiedliche Sicherungszeitpläne zuweisen.

   Wenn Sie 2:00 Uhr morgens geplant haben, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

   a. Führen Sie im Abschnitt „Snapshot-Einstellungen“ die folgenden Aktionen aus:

Wenn Sie wollen…	Dann…
Behalten Sie eine bestimmte Anzahl von Schnappschüssen	Wählen Sie **Zu behaltende Kopien** und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.
Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf	Wählen Sie **Kopien aufbewahren für** und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden.
Sperrzeitraum für Snapshot-Kopien	Wählen Sie **Sperrzeitraum für Snapshot-Kopien** und geben Sie Tage, Monate oder Jahre an. Die Aufbewahrungsdauer von Snaplock sollte weniger als 100 Jahre betragen.

   Für Snapshot-Kopien-basierte Backups müssen Sie die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault -Replikation aktivieren möchten. Wenn Sie die Aufbewahrungsanzahl auf 1 setzen, schlägt der Aufbewahrungsvorgang möglicherweise fehl, da der erste Snapshot der Referenz-Snapshot für die SnapVault -Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

   b. Geben Sie die Richtlinienbezeichnung an.

   Sie können primären Snapshots SnapMirror Labels für die Remote-Replikation zuweisen, sodass die primären Snapshots den Snapshot-Replikationsvorgang von SnapCenter auf sekundäre ONTAP -Systeme auslagern können. Dies kann erfolgen, ohne die Option SnapMirror oder SnapVault auf der Richtlinienseite zu aktivieren.

7. Wählen Sie im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden sekundären Replikationsoptionen aus:

Für dieses Feld…	Machen Sie Folgendes…
Aktualisieren Sie SnapMirror , nachdem Sie eine lokale Snapshot-Kopie erstellt haben	Wählen Sie dieses Feld aus, um Spiegelkopien der Sicherungssätze auf einem anderen Volume zu erstellen (SnapMirror -Replikation). Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden.
Aktualisieren Sie SnapVault , nachdem Sie eine lokale Snapshot-Kopie erstellt haben	Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen (SnapVault -Backups).
Fehleranzahl der Wiederholungsversuche	Geben Sie die maximale Anzahl an Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Erstellen von Ressourcengruppen und Anfügen von Richtlinien

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft sind, gleichzeitig sichern. Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um den Typ des Datenschutzjobs zu definieren, den Sie ausführen möchten.

Informationen zu diesem Vorgang

- Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Klicken Sie auf der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

Für dieses Feld…	Machen Sie Folgendes…
Name	Geben Sie einen Namen für die Ressourcengruppe ein. Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.
Schlagwörter	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.
Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden	Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten. Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

4. Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und einen Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.

   Dies hilft, Informationen auf dem Bildschirm zu filtern.

5. Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:

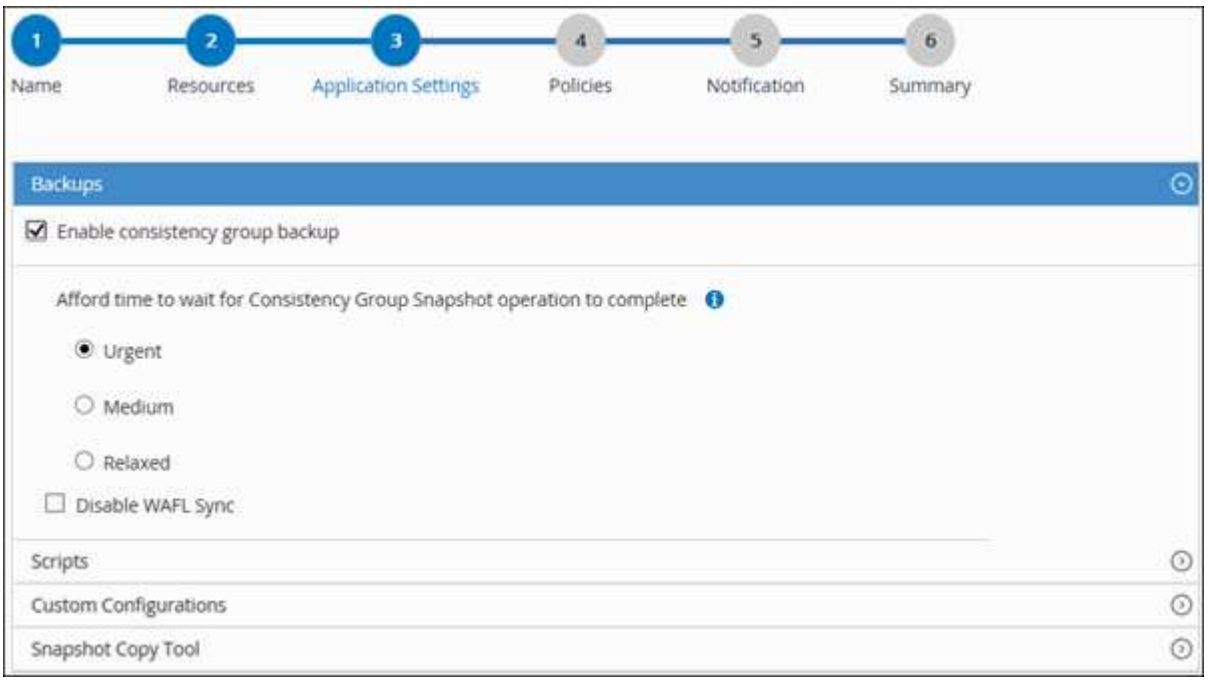
   a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

      Aktivieren Sie die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Machen Sie Folgendes…
Planen Sie Zeit ein, um auf den Abschluss des Snapshot-Vorgangs der Konsistenzgruppe zu warten	Wählen Sie **Dringend**, **Mittel** oder **Entspannt** aus, um die Wartezeit für den Abschluss des Snapshot-Vorgangs anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden.

Für dieses Feld…	Machen Sie Folgendes…
WAFL -Synchronisierung deaktivieren	Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden.

+



a. Klicken Sie auf den Pfeil **Skripts** und geben Sie die Pre- und Post-Befehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge ein. Sie können auch die Vorbefehle eingeben, die im Falle eines Fehlers vor dem Beenden ausgeführt werden sollen.

b. Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie die benutzerdefinierten Schlüssel-Wert-Paare ein, die für alle Datenschutzvorgänge mit dieser Ressource erforderlich sind.

Parameter	Einstellung	Beschreibung
ARCHIV_LOG_ENABLE	(J/N)	Aktiviert die Archivprotokollverwaltung zum Löschen der Archivprotokolle.
ARCHIV_LOG_RETENTION	Anzahl_der_Tage	Gibt die Anzahl der Tage an, für die die Archivprotokolle aufbewahrt werden. Diese Einstellung muss gleich oder größer als NTAP_SNAPSHOT_RETENTIONS sein.
ARCHIVE_LOG_DIR	change_info_directory/logs	Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_EXT	Dateierweiterung	Gibt die Erweiterungslänge der Archivprotokolldatei an. Wenn das Archivprotokoll beispielsweise log_backup_0_0_0_0.16151855 1942 9 lautet und der Wert für die Dateierweiterung 5 ist, behält die Erweiterung des Protokolls 5 Ziffern bei, also 16151.
ARCHIVE_LOG_RECURSIVE_ SE ARCH	(J/N)	Ermöglicht die Verwaltung von Archivprotokollen in Unterverzeichnissen. Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle in Unterverzeichnissen befinden.

Die benutzerdefinierten Schlüssel-Wert-Paare werden für IBM Db2 Linux-Plug-in-Systeme unterstützt, jedoch nicht für IBM Db2-Datenbanken, die als zentrales Windows-Plug-in registriert sind.

c. Klicken Sie auf den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

Falls Sie es wollen…	Dann…
SnapCenter , um das Plug-In für Windows zu verwenden und das Dateisystem in einen konsistenten Zustand zu versetzen, bevor ein Snapshot erstellt wird. Für Linux-Ressourcen ist diese Option nicht anwendbar.	Wählen Sie * SnapCenter mit Dateisystemkonsistenz*.
SnapCenter zum Erstellen eines Snapshots auf Speicherebene	Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.
Geben Sie den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot-Kopien zu erstellen.	Wählen Sie **Andere** aus und geben Sie dann den Befehl ein, der auf dem Host ausgeführt werden soll, um einen Snapshot zu erstellen.

7. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.

Sie können auch eine Richtlinie erstellen, indem Sie auf * klicken. + *.

Die Richtlinien sind im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgeführt.

b. Klicken Sie in der Spalte „Zeitpläne konfigurieren“ auf * + * für die Richtlinie, die Sie konfigurieren möchten.

c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

Dabei ist „policy_name“ der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne werden in der Spalte **Angewandte Zeitpläne** aufgelistet.

Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

   Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Der SMTP-Server muss unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für IBM Db2-Ressourcen auf ASA r2-Systemen

Sie sollten die Ressourcengruppe erstellen, um die Ressourcen hinzuzufügen, die sich auf ASA R2-Systemen befinden. Sie können den sekundären Schutz auch beim Erstellen der Ressourcengruppe bereitstellen.

Bevor Sie beginnen

- Sie sollten sicherstellen, dass Sie nicht sowohl ONTAP 9.x-Ressourcen als auch ASA r2-Ressourcen zur gleichen Ressourcengruppe hinzufügen.
- Sie sollten sicherstellen, dass Sie keine Datenbank mit ONTAP 9.x-Ressourcen und ASA r2-Ressourcen haben.

Informationen zu diesem Vorgang

- Der sekundäre Schutz ist nur verfügbar, wenn dem angemeldeten Benutzer die Rolle zugewiesen ist, für die die Funktion **SecondaryProtection** aktiviert ist.
- Wenn Sie den sekundären Schutz aktiviert haben, wird die Ressourcengruppe beim Erstellen der primären und sekundären Konsistenzgruppen in den Wartungsmodus versetzt. Nachdem die primäre und sekundäre Konsistenzgruppe erstellt wurden, wird der Wartungsmodus der Ressourcengruppe beendet.
- SnapCenter unterstützt keinen sekundären Schutz für eine Klonressource.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-In aus der Liste aus.
2. Klicken Sie auf der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

a. Geben Sie im Feld „Name“ einen Namen für die Ressourcengruppe ein.

   Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.

b. Geben Sie im Feld „Tag“ eine oder mehrere Bezeichnungen ein, um die spätere Suche nach der Ressourcengruppe zu erleichtern.

   Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.

c. Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

   Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

d. Geben Sie die Ziele der Archivprotokolldateien an, die Sie nicht sichern möchten.

   Sie sollten genau dasselbe Ziel verwenden, das in der Anwendung festgelegt wurde, gegebenenfalls einschließlich Präfix.

4. Wählen Sie auf der Seite „Ressourcen“ den Datenbank-Hostnamen aus der Dropdown-Liste **Host** aus.

   Die Ressourcen werden nur dann im Abschnitt „Verfügbare Ressourcen“ aufgeführt, wenn die Ressource erfolgreich erkannt wurde. Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

5. Wählen Sie die ASA r2-Ressourcen aus dem Abschnitt „Verfügbare Ressourcen“ aus und verschieben Sie sie in den Abschnitt „Ausgewählte Ressourcen“.
6. Wählen Sie auf der Seite „Anwendungseinstellungen“ die Sicherungsoption aus.
7. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.

      Sie können eine Richtlinie auch erstellen, indem Sie auf + .

      Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

   b. Klicken + in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

   c. Konfigurieren Sie im Fenster „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

      Dabei ist *Richtlinienname* der Name der von Ihnen ausgewählten Richtlinie.

      Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von

SnapCenter überschneiden.

8. Wenn der sekundäre Schutz für die von Ihnen ausgewählte Richtlinie aktiviert ist, wird die Seite „Sekundärer Schutz“ angezeigt und Sie müssen die folgenden Schritte ausführen:
   a. Wählen Sie den Typ der Replikationsrichtlinie aus.

      Die synchrone Replikationsrichtlinie wird nicht unterstützt.

   b. Geben Sie das Konsistenzgruppensuffix an, das Sie verwenden möchten.
   c. Wählen Sie aus den Dropdown-Menüs „Zielcluster“ und „Ziel-SVM“ den Peering-Cluster und die SVM aus, die Sie verwenden möchten.

      Das Cluster- und SVM-Peering wird von SnapCenter nicht unterstützt. Sie sollten System Manager oder ONTAP CLIs verwenden, um Cluster- und SVM-Peering durchzuführen.

Wenn die Ressourcen bereits außerhalb von SnapCenter geschützt sind, werden diese Ressourcen im Abschnitt „Sekundär geschützte Ressourcen“ angezeigt.

1. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:
   a. Klicken Sie auf **Locators laden**, um die SnapMirror oder SnapVault -Volumes zu laden und die Überprüfung auf dem sekundären Speicher durchzuführen.
   b. Klicken + in der Spalte „Zeitpläne konfigurieren“, um den Überprüfungszeitplan für alle Zeitplantypen der Richtlinie zu konfigurieren.
   c. Führen Sie im Dialogfeld „Verifizierungszeitpläne hinzufügen“ (Richtlinienname) die folgenden Aktionen aus:

Wenn Sie wollen…	Machen Sie Folgendes…
Führen Sie nach der Sicherung eine Überprüfung durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planen Sie eine Überprüfung	Wählen Sie **Geplante Überprüfung ausführen** und wählen Sie dann den Zeitplantyp aus der Dropdownliste aus.

   d. Wählen Sie **Am sekundären Speicherort überprüfen**, um Ihre Sicherungen auf dem sekundären Speichersystem zu überprüfen.
   e. Klicken Sie auf **OK**.

      Die konfigurierten Überprüfungszeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

2. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

   Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den an der Ressourcengruppe durchgeführten Vorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.

Für die E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder über die GUI oder den PowerShell-Befehl „Set-SmSmtpServer“ angegeben haben.

3. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets für IBM Db2

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Sichern, Wiederherstellen oder Klonen von IBM Db2-Datenbanken verwenden.

Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

  Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Daten-LIF-IP-Adresse haben.

Schritte

1. Klicken Sie auf **SnapCenterPS**, um PowerShell Core zu starten.
2. Erstellen Sie mithilfe des Cmdlets Add-SmStorageConnection eine neue Verbindung zum Speichersystem.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Erstellen Sie mithilfe des Cmdlets Add-SmCredential neue Anmeldeinformationen.

   Dieses Beispiel zeigt, wie Sie mit Windows-Anmeldeinformationen neue Anmeldeinformationen mit dem Namen „FinanceAdmin“ erstellen:

```
PS C:\> Add-SmCredential -Name 'FinanceAdmin' -Type Linux
-AuthenticationType PasswordBased -Credential db2hostuser
-EnableSudoPrevileges:$true
```

4. Fügen Sie den IBM Db2-Kommunikationshost zum SnapCenter Server hinzu.

   Für Linux:

   ```
   PS C:\> Add-SmHost -HostType Linux -HostName '10.232.204.61'
   -CredentialName 'defaultcreds'
   ```

   Für Windows:

   ```
   PS C:\> Add-SmHost -HostType Windows -HostName '10.232.204.61'
   -CredentialName 'defaultcreds'
   ```

5. Installieren Sie das Paket und das SnapCenter -Plug-in für IBM Db2 auf dem Host.

   Für Linux:

   ```
   PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
   DB2
   ```

   Für Windows:

   ```
   PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
   DB2,SCW
   ```

6. Legen Sie den Pfad zur SQLLIB fest.

   Für Windows verwendet das Db2-Plug-In den Standardpfad für den SQLLIB-Ordner: „C:\Programme\IBM\SQLLIB\BIN“.

   Wenn Sie den Standardpfad überschreiben möchten, verwenden Sie den folgenden Befehl.

   ```
   PS C:\> Set-SmConfigSettings -Plugin -HostName '10.232.204.61'
   -PluginCode DB2 -configSettings
   @{"DB2_SQLLIB_CMD"="<custom_path>\IBM\SQLLIB\BIN"}
   ```

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Sichern von Db2-Datenbanken

Das Sichern einer Datenbank umfasst das Herstellen einer Verbindung mit dem SnapCenter -Server, das Hinzufügen von Ressourcen, das Hinzufügen einer Richtlinie,

das Erstellen einer Sicherungsressourcengruppe und das Sichern.

Bevor Sie beginnen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Stellen Sie bei Sicherungsvorgängen auf Basis von Snapshot-Kopien sicher, dass alle Mandantendatenbanken gültig und aktiv sind.
- Bei Pre- und Post-Befehlen für Quiesce-, Snapshot- und Unquiesce-Vorgänge sollten Sie überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host unter den folgenden Pfaden verfügbar ist:
  - Standardspeicherort auf dem Windows-Host: *C:\Programme\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Standardspeicherort auf dem Linux-Host: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Wenn die Befehle nicht in der Befehlsliste vorhanden sind, schlägt der Vorgang fehl.

SnapCenter -Benutzeroberfläche

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Ressourcenseite die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.

   Wählen und wählen Sie dann den Hostnamen und den Ressourcentyp aus, um die Ressourcen zu filtern. Sie können dann auswählen , um den Filterbereich zu schließen.
3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Ressourcenseite **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

   Beispiel: *customtext_policy_hostname* oder *resource_hostname*. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.
5. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:

   - Wählen Sie den Pfeil **Backups** aus, um zusätzliche Backup-Optionen festzulegen:

     Aktivieren Sie bei Bedarf die Konsistenzgruppensicherung und führen Sie die folgenden Aufgaben aus:

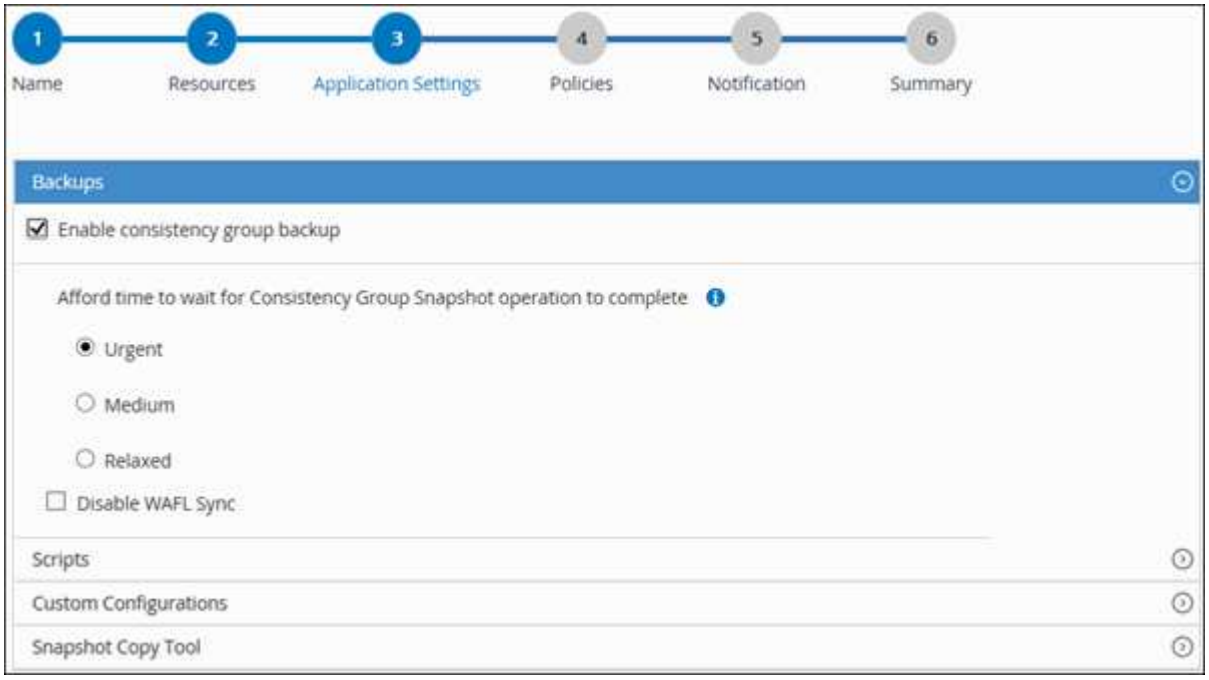
Für dieses Feld…	Machen Sie Folgendes…
Planen Sie Zeit ein, um auf den Abschluss des Vorgangs „Consistency Group Snapshot“ zu warten	Wählen Sie **Dringend**, **Mittel** oder **Entspannt** aus, um die Wartezeit für die Fertigstellung des Snapshot-Vorgangs festzulegen. Dringend = 5 Sekunden, Mittel = 7 Sekunden und Entspannt = 20 Sekunden.
WAFL -Synchronisierung deaktivieren	Wählen Sie diese Option, um das Erzwingen eines WAFL Konsistenzpunkts zu vermeiden.

   - Wählen Sie den Pfeil **Skripts** aus, um Vor- und Nachbefehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge auszuführen.

     Sie können vor dem Beenden des Sicherungsvorgangs auch Vorbefehle ausführen. Prescripts und Postscripts werden auf dem SnapCenter -Server ausgeführt.

   - Wählen Sie den Pfeil **Benutzerdefinierte Konfigurationen** aus und geben Sie dann die benutzerdefinierten Wertepaare ein, die für alle Jobs erforderlich sind, die diese Ressource verwenden.
   - Wählen Sie den Pfeil **Snapshot-Kopiertool**, um das Tool zum Erstellen von Snapshots auszuwählen:

Falls Sie es wollen…	Dann…
SnapCenter zum Erstellen eines Snapshots auf Speicherebene	Wählen Sie * SnapCenter ohne Dateisystemkonsistenz*.
SnapCenter , um das Plug-In für Windows zu verwenden, um das Dateisystem in einen konsistenten Zustand zu versetzen und dann einen Snapshot zu erstellen	Wählen Sie * SnapCenter mit Dateisystemkonsistenz*.
So geben Sie den Befehl zum Erstellen eines Snapshots ein	Wählen Sie **Andere** und geben Sie dann den Befehl zum Erstellen eines Snapshots ein.



6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.

      Sie können auch eine Richtlinie erstellen, indem Sie auf * klicken. + *.

      Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

   b. Wählen * + * in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

   c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan und wählen Sie dann **OK** aus.

      policy_name ist der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

7. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

   Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. SMTP muss auch unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

8. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.

   Die Seite mit der Ressourcentopologie wird angezeigt.

9. Wählen Sie **Jetzt sichern**.
10. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
    a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

       Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.

    b. Wählen Sie **Backup**.
11. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.
    - In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung erkennen.

      Weitere Informationen finden Sie unter: "SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"

PowerShell-Cmdlets

Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

```
PS C:\> Open-SmConnection
```

   Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

2. Fügen Sie mithilfe des Cmdlets Add-SmResources manuelle Ressourcen hinzu.

   Dieses Beispiel zeigt, wie eine IBM Db2-Instanz hinzugefügt wird:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Instance -ResourceName db2inst1 -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"Stora
geSystem"="scsnfssvm"}) -MountPoints "D:\"
```

   Für die Db2-Datenbank:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Database -ResourceName SALESDB -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"Stora
geSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

3. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets Add-SmPolicy.
4. Schützen Sie die Ressource oder fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.
5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

   Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert wird:

   ```
   C:\PS> New-SMBackup -ResourceGroupName
   'ResourceGroup_with_Db2_Resources' -Policy db2_policy1
   ```

   In diesem Beispiel wird eine Db2-Instanz gesichert:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.32.212.13";"Uid"="DB2INST1";"PluginName"="DB2"} -Policy
   db2_policy
   ```

   In diesem Beispiel wird eine Db2-Datenbank gesichert:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCDB";"PluginName"="DB2"
   } -Policy db2_policy
   ```

6. Überwachen Sie den Auftragsstatus (wird ausgeführt, abgeschlossen oder fehlgeschlagen) mithilfe des Cmdlets Get-smJobSummaryReport.

```
PS C:\> Get-SmJobSummaryReport -JobId 467

SmJobId            : 467
JobCreatedDateTime :
JobStartDateTime   : 27-Jun-24 01:40:09
JobEndDateTime     : 27-Jun-24 01:41:15
JobDuration        : 00:01:06.7013330
JobName            : Backup of Resource Group
'SCDB201WIN_RAVIR1_OPENLAB_NETAPP_LOCAL_DB2_DB2_WINCIR' with policy
'snapshot-based-db2'
JobDescription     :
Status             : Completed
IsScheduled        : False
JobError           :
JobType            : Backup
PolicyName         : db2_policy
JobResultData      :
```

7. Überwachen Sie die Details des Sicherungsauftrags wie Sicherungs-ID und Sicherungsname, um mithilfe des Cmdlets Get-SmBackupReport Wiederherstellungs- oder Klonvorgänge durchzuführen.

```
PS C:\> Get-SmBackupReport -JobId 467

BackedUpObjects           : {WINCIR}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 84
SmJobId                   : 467
StartDateTime             : 27-Jun-24 01:40:09
EndDateTime               : 27-Jun-24 01:41:15
Duration                  : 00:01:06.7013330
CreatedDateTime           : 27-Jun-24 18:39:45
Status                    : Completed
ProtectionGroupName       : HOSTFQDN_DB2_DB2_WINCIR
SmProtectionGroupId       : 23
PolicyName                : db2_policy
SmPolicyId                : 13
BackupName                : HOSTFQDN _DB2_DB2_WINCIR_HOST_06-27-
2024_01.40.09.7397
VerificationStatus        : NotApplicable
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
PluginCode                : SCC
PluginName                : DB2
PluginDisplayName         : IBM DB2
JobTypeId                 :
JobHost                   : HOSTFQDN
```

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Sichern von Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.

- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.

Informationen zu diesem Vorgang

Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Anzeigen“ die Option „Ressourcengruppe“ aus.

   Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder indem Sie und wählen Sie dann das Tag aus. Sie können dann auswählen , um den Filterbereich zu schließen.
3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und wählen Sie dann **Jetzt sichern** aus.
4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

      Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.

   b. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

Überwachen von IBM Db2-Sicherungsvorgängen

Sie können den Fortschritt verschiedener Sicherungsvorgänge mithilfe der SnapCenterJobs-Seite überwachen. Möglicherweise möchten Sie den Fortschritt überprüfen, um festzustellen, wann der Vorgang abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und zeigen den entsprechenden Status der Vorgänge an:

- Im Gange
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden

- In der Warteschlange
- Abgesagt

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite „Überwachen“ auf **Jobs**.
3. Führen Sie auf der Seite „Jobs“ die folgenden Schritte aus:
   a. Klicken um die Liste so zu filtern, dass nur Sicherungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdownliste **Typ** die Option **Backup** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Sicherungsstatus aus.
   e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.

   Obwohl der Status des Sicherungsauftrags angezeigt wird Wenn Sie auf die Auftragsdetails klicken, sehen Sie möglicherweise, dass einige der untergeordneten Aufgaben des Sicherungsvorgangs noch ausgeführt werden oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite „Auftragsdetails“ auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Überwachen Sie Datenschutzvorgänge für IBM Db2-Datenbanken im Aktivitätsbereich

Im Aktivitätsbereich werden die fünf zuletzt ausgeführten Vorgänge angezeigt. Im Aktivitätsbereich wird auch angezeigt, wann der Vorgang gestartet wurde und welchen Status er hat.

Im Aktivitätsbereich werden Informationen zu Sicherungs-, Wiederherstellungs-, Klon- und geplanten Sicherungsvorgängen angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Klicken im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.

   Wenn Sie auf einen der Vorgänge klicken, werden die Vorgangsdetails auf der Seite **Auftragsdetails** aufgelistet.

Abbrechen von Sicherungsvorgängen für IBM Db2

Sie können Sicherungsvorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die Sicherungsvorgänge über die SnapCenter -GUI, PowerShell-Cmdlets oder CLI-Befehle abbrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitorseite	a. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. b. Wählen Sie den Vorgang aus und klicken Sie dann auf **Auftrag abbrechen**.
Aktivitätsbereich	a. Klicken Sie nach dem Starten des Sicherungsvorgangs auf * * im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite „Auftragsdetails“ auf **Auftrag abbrechen**.

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt.

Anzeigen von IBM Db2-Sicherungen und -Klonen auf der Seite „Topologie“

Wenn Sie die Sicherung oder das Klonen einer Ressource vorbereiten, kann es hilfreich sein, eine grafische Darstellung aller Sicherungen und Klone auf dem primären und sekundären Speicher anzuzeigen.

Informationen zu diesem Vorgang

Sie können die folgenden Symbole in der Ansicht „Kopien verwalten“ überprüfen, um festzustellen, ob die Sicherungen und Klone auf dem primären oder sekundären Speicher verfügbar sind (Spiegelkopien oder Tresorkopien).

-

 zeigt die Anzahl der Backups und Klone an, die auf dem primären Speicher verfügbar sind.

-  zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapMirror -Technologie auf dem sekundären Speicher gespiegelt werden.
-  zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapVault -Technologie auf dem sekundären Speicher repliziert werden.

Die angezeigte Anzahl der Backups umfasst die aus dem sekundären Speicher gelöschten Backups. Wenn Sie beispielsweise 6 Sicherungen mit einer Richtlinie zum Aufbewahren von nur 4 Sicherungen erstellt haben, wird die Anzahl der angezeigten Sicherungen mit 6 angegeben.

Klone einer Sicherung eines versionsflexiblen Spiegels auf einem Volume vom Typ „Mirror-Vault“ werden in der Topologieansicht angezeigt, die Anzahl der Spiegelsicherungen in der Topologieansicht umfasst jedoch nicht die versionsflexible Sicherung.

Auf der Seite „Topologie“ können Sie alle Sicherungen und Klone sehen, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details dieser Sicherungen und Klone anzeigen und sie dann auswählen, um Datenschutzvorgänge durchzuführen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ entweder die Ressource oder die Ressourcengruppe aus der Dropdownliste **Anzeigen** aus.
3. Wählen Sie die Ressource entweder aus der Ressourcendetailansicht oder aus der Ressourcengruppendetailansicht aus.

   Wenn die Ressource geschützt ist, wird die Topologieseite der ausgewählten Ressource angezeigt.

4. Überprüfen Sie die **Zusammenfassungskarte**, um eine Zusammenfassung der Anzahl der auf dem primären und sekundären Speicher verfügbaren Backups und Klone anzuzeigen.

   Der Abschnitt **Zusammenfassungskarte** zeigt die Gesamtzahl der auf Snapshot-Kopien basierenden Backups und Klone an.

   Durch Klicken auf die Schaltfläche **Aktualisieren** wird eine Abfrage des Speichers gestartet, um eine genaue Anzahl anzuzeigen.

   Wenn eine SnapLock -fähige Sicherung durchgeführt wird, wird durch Klicken auf die Schaltfläche **Aktualisieren** die von ONTAP abgerufene Ablaufzeit des primären und sekundären SnapLock aktualisiert. Ein wöchentlicher Zeitplan aktualisiert auch die von ONTAP abgerufene Ablaufzeit des primären und sekundären SnapLock .

   Wenn die Anwendungsressource auf mehrere Volumes verteilt ist, entspricht die SnapLock -Ablaufzeit für die Sicherung der längsten SnapLock -Ablaufzeit, die für einen Snapshot in einem Volume festgelegt ist.

Die längste SnapLock -Ablaufzeit wird von ONTAP abgerufen.

Nach der On-Demand-Sicherung werden durch Klicken auf die Schaltfläche **Aktualisieren** die Details der Sicherung oder des Klons aktualisiert.

5. Klicken Sie in der Ansicht „Kopien verwalten“ auf **Backups** oder **Klone** vom primären oder sekundären Speicher, um Details zu einem Backup oder Klon anzuzeigen.

   Die Details der Backups und Klone werden in einem Tabellenformat angezeigt.

6. Wählen Sie die Sicherung aus der Tabelle aus und klicken Sie dann auf die Datenschutzsymbole, um Wiederherstellungs-, Klon- und Löschvorgänge durchzuführen.

   Sie können Sicherungen, die sich auf dem sekundären Speicher befinden, weder umbenennen noch löschen.

7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .
8. Wenn Sie einen Klon teilen möchten, wählen Sie den Klon aus der Tabelle aus und klicken Sie dann auf .