



SnapCenter software ドキュメント

SnapCenter software

NetApp
September 29, 2025

This PDF was generated from <https://docs.netapp.com/ja-jp/snapcenter-61/index.html> on September 29, 2025. Always check docs.netapp.com for the latest.

目次

SnapCenter software ドキュメント	1
リリース ノート	2
リリース ノート	2
SnapCenterでサポートされているアップグレード パス	2
始めましょう	3
SnapCenter softwareについて学ぶ	3
SnapCenterの概要	3
SnapCenterのセキュリティ機能	8
SnapCenterのロールベースのアクセス制御	9
SnapCenterでの災害復旧	14
SnapCenterに必要なライセンス	15
SnapCenterのSnapMirrorアクティブ同期	18
データ保護の主要概念	19
SnapCenterでサポートされるストレージ システムとアプリケーション	21
SnapCenter資格情報の認証方法	22
ASA r2 システムでサポートされているSnapCenter操作	23
SnapCenter softwareのクイック スタート	24
SnapCenter Serverのインストールと構成	26
SnapCenter Serverのインストールの準備	26
SnapCenter Server をインストールするための要件	26
SnapCenterソフトウェアにアクセスするための登録	32
多要素認証 (MFA)	33
SnapCenter Serverのインストール	43
WindowsホストへのSnapCenter Serverのインストール	43
LinuxホストへのSnapCenter Serverのインストール	47
SnapCenterを登録する	51
RBAC許可を使用したSnapCenterへのログイン	51
SnapCenterサーバーを構成する	55
ストレージシステムの追加とプロビジョニング	55
SnapCenter Standardコントローラベース ライセンスの追加	77
高可用性の設定	82
ロールベース アクセス制御 (RBAC) の設定	86
監査ログの設定	115
SnapCenter ServerとのセキュアなMySQL接続の設定	116
証明書ベースの認証を構成する	122
証明書ベースの認証の有効化	122
SnapCenter Serverからの認証局 (CA) 証明書のエクスポート	122
WindowsプラグインホストにCA証明書をインポートする	123
UNIXプラグイン ホストへのCA証明書のインポート	124

SnapCenter証明書のエクスポート	125
WindowsホストのCA証明書の設定	126
CA証明書CSRファイルの生成	126
CA証明書のインポート	127
CA証明書のサムプリントの取得	127
Windowsホスト プラグイン サービスでのCA証明書の設定	128
SnapCenterサイトでのCA証明書の設定	129
SnapCenterのCA証明書の有効化	129
LinuxホストのCA証明書の設定	130
nginx証明書の設定	130
監査ログ証明書の設定	130
SnapCenterサービス証明書の設定	131
Windowsホストでの双方向SSL通信の設定と有効化	131
Windowsホストでの双方向SSL通信の設定	131
Windowsホストでの双方向SSL通信の有効化	134
Linuxホストでの双方向SSL通信の設定と有効化	135
Linuxホストでの双方向SSL通信の設定	135
LinuxホストでのSSL通信の有効化	137
Active Directory、LDAP、LDAPSの設定	137
信頼されていないActive Directoryドメインの登録	137
Active Directoryの読み取り権限を有効にするためのIISアプリケーション プールの設定	139
LDAPS用のCAクライアント証明書の設定	140
Microsoft SQL Serverデータベースの保護	141
SnapCenter Plug-in for Microsoft SQL Server	141
SnapCenter Plug-in for Microsoft SQL Serverの概要	141
SnapCenter Plug-in for Microsoft SQL Serverの機能	141
SnapCenter Plug-in for Microsoft SQL Serverの特長	142
Windowsクラスタでの非対称LUNマッピングのサポート	143
SnapCenter Plug-in for Microsoft SQL Serverでサポートされるストレージ タイプ	144
SnapCenter Plug-in for Microsoft SQL Serverのストレージ レイアウトに関する推奨事項	147
SQLプラグインに必要な最小ONTAP権限	149
Plug-in for SQL ServerのSnapMirrorレプリケーションとSnapVaultレプリケーション用のストレージ システムを準備する	151
SQL Serverリソースのバックアップ戦略	152
SQL Serverのリストア戦略	156
SQL Serverのクローニング戦略の定義	160
SnapCenter Plug-in for Microsoft SQL Serverのインストール準備	160
SnapCenter Plug-in for Microsoft SQL Serverのインストール ワークフロー	160
ホストを追加してSnapCenter Plug-in for Microsoft SQL Serverをインストールするための前提条件	161
SnapCenter Plug-ins Package for Windowsをインストールするホストの要件	162
SnapCenter Plug-ins Package for Windowsのクレデンシャルの設定	163

個々のSQL Serverリソースのクレデンシャルの設定	164
Windows Server 2016以降でのgMSAの設定	166
SnapCenter Plug-in for Microsoft SQL Serverのインストール	168
CA証明書の設定	174
ディザスタ リカバリの設定	177
SnapCenter Plug-in for VMware vSphereのインストール	179
CA証明書を導入する	180
CRLファイルを設定する	180
データ保護の準備	180
SnapCenter Plug-in for Microsoft SQL Serverを使用するための前提条件	180
SQL Serverの保護におけるソース、リソース グループ、ポリシーの使用方法	181
SQL Serverのデータベース、インスタンス、可用性グループのバックアップ	182
バックアップのワークフロー	182
リソースをバックアップに使用できるかどうかの確認	183
NetAppストレージ システムへのリソースの移行	185
SQL Serverデータベースのバックアップ ポリシーの作成	187
SQL Serverに対するリソース グループの作成とポリシーの適用	193
リソース グループを作成し、ASA r2 システム上の Microsoft SQL Server	196
リソースの二次保護を有効にします。	
SQLリソースのバックアップの要件	199
PowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成	199
SQLリソースのバックアップ	200
SQL Serverリソース グループのバックアップ	206
SnapCenterの[Jobs]ページでのSQLリソースのバックアップ処理の監視	207
SnapCenter Plug-in for Microsoft SQL Serverのバックアップ処理のキャンセル	208
[Topology]ページでのSQL Serverのバックアップとクローンの表示	209
PowerShellコマンドレットを使用したセカンダリ バックアップ数のクリーンアップ	211
SQL Serverリソースのリストア	212
リストアのワークフロー	212
データベースをリストアする際の要件	212
SQL Serverデータベースのバックライトのリストア	213
セカンダリ ストレージからSQL Serverデータベースのリストア	220
PowerShellコマンドレットを使用したリソースのリストア	221
可用性グループ データベースの再シード	224
SQLリソースのリストア処理の監視	225
SQLリソースのリストア処理のキャンセル	226
SQL Serverデータベース リソースのクローニング	227
クローニングのワークフロー	227
SQL Serverデータベース バックアップからのクローニング	227
クローン ライフサイクルの実行	235
SQLデータベースのクローニング処理の監視	238

SQLリソースのクローニング処理のキャンセル	239
クローンのスプリット	239
SAP HANAデータベースの保護	241
SnapCenter Plug-in for SAP HANA Database	241
SnapCenter Plug-in for SAP HANA Databaseの概要	241
SnapCenter Plug-in for SAP HANA Databaseの機能	241
SnapCenter Plug-in for SAP HANA Databaseの特長	241
SnapCenter Plug-in for SAP HANA Databaseでサポートされるストレージ タイプ	242
SAP HANAプラグインに必要な最小ONTAP権限	243
SAP HANAデータベースでのSnapMirrorレプリケーションと SnapVaultレプリケーションのためのストレージ システムの準備	246
SAP HANAデータベースのバックアップ戦略	246
SAP HANAデータベースのリストアとリカバリの戦略	250
SnapCenter Plug-in for SAP HANA Databaseのインストール準備	252
SnapCenter Plug-in for SAP HANA Databaseのインストール ワークフロー	252
ホストを追加してSnapCenter Plug-in for SAP HANA Databaseをインストールするための前提条件	253
SnapCenter Plug-ins Package for Windowsをインストールするホストの要件	256
SnapCenter Plug-ins Package for Linuxをインストールするホストの要件	257
SnapCenter Plug-in for SAP HANA Databaseのクレデンシャルの設定	258
Windows Server 2016以降でのgMSAの設定	261
SnapCenter Plug-in for SAP HANA Databaseのインストール	262
CA証明書の設定	268
SnapCenter Plug-in for VMware vSphereのインストール	276
CA証明書を導入する	276
CRLファイルを設定する	276
データ保護の準備	276
SnapCenter Plug-in for SAP HANA Databaseを使用するための前提条件	276
SAP HANAデータベースの保護におけるリソース、リソース グループ、ポリシーの使用方法	277
SAP HANAリソースのバックアップ	278
SAP HANAリソースのバックアップ	278
SAP HANAデータベースのHDBユーザ ストア キーとHDBSQL OSユーザの設定	279
データ保護のためのリソースの検出とマルチテナント データベース コンテナの準備	280
手動でのプラグイン ホストへのリソースの追加	282
SAP HANAデータベースのバックアップ ポリシーの作成	284
リソース グループの作成とポリシーの適用	289
リソース グループを作成し、ASA r2 システム上の SAP HANA リソースの二次保護を有効にする	293
SAP HANAデータベース用のPowerShellコマンドレットを使用したストレージ システムへの接続とクレデンシャルの作成	296
SAP HANAデータベースのバックアップ	298
リソース グループのバックアップ	305
SAP HANAデータベースのバックアップ処理の監視	305

SAP HANAのバックアップ処理のキャンセル	306
[Topology]ページでのSAP HANAデータベースのバックアップとクローンの表示	307
SAP HANAデータベースのリストア	309
リストアのワークフロー	309
手動で追加されたリソース バックアップのリストアとリカバリ	310
自動検出されたデータベース バックアップのリストアとリカバリ	314
PowerShellコマンドレットを使用したリソースのリストア	318
SAP HANAデータベースのリストア処理の監視	320
SAP HANAリソースのバックアップのクローニング	321
クローニングのワークフロー	321
SAP HANAデータベースのバックアップのクローニング	322
SAP HANAデータベースのクローニング処理の監視	326
クローンのスプリット	326
SnapCenterアップグレード後のSAP HANAデータベースのクローンの削除またはスプリット	328
Oracleデータベースの保護	329
SnapCenter Plug-in for Oracle Databaseの概要	329
Plug-in for Oracle Databaseの機能	329
Plug-in for Oracle Databaseの機能	329
Plug-in for Oracle Databaseでサポートされるストレージ タイプ	331
Plug-in for OracleでのSnapMirrorレプリケーションと SnapVaultレプリケーションのためのストレージ システムの準備	333
Plug-in for Oracleに必要な最小限のONTAP権限	334
SnapCenter Plug-in for Oracle Databaseのインストール	336
SnapCenter Plug-in for Oracle Databaseのインストール ワークフロー	336
ホストを追加してPlug-in Package for Linux / AIXをインストールするための前提条件	336
GUIを使用してホストを追加し、Plug-ins Package for Linux / AIXをインストールする	345
LinuxまたはAIX用のプラグイン パッケージをインストールする別の方法	349
SnapCenter Plug-in Loaderサービスの設定	352
LinuxホストでのSnapCenter Plug-in Loader (SPL) サービスを使用したCA証明書の設定	355
プラグインのCA証明書の有効化	358
SnapManager for OracleおよびSnapManager for SAPからのSnapCenterへのデータのインポート	359
SnapCenter Plug-in for VMware vSphereのインストール	364
CA証明書を導入する	365
CRLファイルを設定する	365
Oracleデータベースの保護の準備	365
Oracleデータベースのバックアップ	366
バックアップ手順の概要	367
バックアップ構成情報	368
Oracleデータベースのバックアップの要件	380
バックアップに使用できるOracleデータベースの検出	381
Oracleデータベースのバックアップ ポリシーの作成	383

Oracleデータベースのリソース グループの作成とポリシーの適用	389
リソース グループを作成し、ASA r2 システム上の Oracle リソースの二次保護を有効にします。	391
Oracleリソースのバックアップ	394
Oracleデータベースのリソース グループのバックアップ	397
Oracleデータベースのバックアップの監視	398
その他のバックアップ処理	399
データベース バックアップのマウントとアンマウント	403
データベース バックアップをマウントする	404
データベース バックアップをアンマウントする	405
Oracleデータベースのリストアとリカバリ	405
リストアのワークフロー	406
Oracleデータベースのリストアおよびリカバリ戦略の定義	406
リストア固有のプリスクリプトとポストスクリプト用に事前定義された環境変数	411
Oracleデータベースをリストアするための要件	412
Oracleデータベースのリストアとリカバリ	413
ポイントインタイム リカバリを使用した表領域のリストアとリカバリ	418
ポイントインタイム リカバリを使用したプラガブル データベースのリストアとリカバリ	420
UNIXコマンドを使用したOracleデータベースのリストアとリカバリ	423
Oracleデータベースのリストア処理の監視	423
Oracleデータベースのリストア処理のキャンセル	424
Oracleデータベースのクローニング	425
クローニングのワークフロー	425
Oracleデータベースのクローニング戦略の定義	426
クローン固有のプリスクリプトとポストスクリプト用に事前定義された環境変数	427
Oracleデータベースをクローニングするための要件	429
Oracleデータベース バックアップのクローニング	431
プラガブル データベースのクローニング	440
UNIXコマンドを使用したOracleデータベース バックアップのクローニング	445
Oracle Databaseクローンのスプリット	445
プラガブル データベースのクローンのスプリット	446
Oracleデータベースのクローニング処理の監視	447
クローンの更新	448
プラガブル データベースのクローンの削除	449
アプリケーション ボリュームの管理	449
アプリケーション ボリュームとは	449
アプリケーション ボリュームの追加	450
アプリケーション ボリュームのバックアップ	451
アプリケーション ボリュームのバックアップのクローニング	454
Windowsファイルシステムの保護	456
SnapCenter Plug-in for Microsoft Windowsの概念	456
SnapCenter Plug-in for Microsoft Windowsの概要	456

SnapCenter Plug-in for Microsoft Windowsの機能	456
SnapCenter Plug-in for Windowsの特長	457
SnapCenterでのWindowsファイルシステムのバックアップ方法	458
SnapCenter Plug-in for Microsoft Windowsでサポートされるストレージ タイプ	458
Windowsプラグインに必要な最小ONTAP権限	461
SnapMirrorレプリケーションとSnapVaultレプリケーションのためのストレージ システムの準備	463
Windowsファイルシステムのバックアップ戦略の定義	464
Windowsファイルシステムのクローンのソースとデスティネーション	466
SnapCenter Plug-in for Microsoft Windowsのインストール	466
SnapCenter Plug-in for Microsoft Windowsのインストール ワークフロー	466
SnapCenter Plug-in for Microsoft Windowsのインストール要件	466
ホストの追加とSnapCenter Plug-in for Microsoft Windowsのインストール	471
PowerShellコマンドレットを使用した複数のリモート ホストへのSnapCenter Plug-in for Microsoft Windowsのインストール	475
コマンドラインからのSnapCenter Plug-in for Microsoft Windowsのサイレント インストール	475
SnapCenterプラグイン パッケージのインストール ステータスの監視	477
CA証明書の設定	478
SnapCenter Plug-in for VMware vSphereのインストール	481
CA証明書を導入する	481
CRLファイルを設定する	481
Windowsファイルシステムのバックアップ	481
Windowsファイルシステムのバックアップ	481
Windowsファイルシステムの使用可能なリソースの確認	483
Windowsファイルシステムのバックアップ ポリシーの作成	484
Windowsファイルシステムのリソース グループの作成	487
ASA r2 システム上の Windows ファイル システムのリソース	489
グループを作成し、二次保護を有効にします。	
PowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成	492
Windowsファイルシステムの単一リソースのオンデマンド バックアップ	493
Windowsファイルシステムのリソース グループのバックアップ	497
バックアップ処理の監視	498
バックアップ処理のキャンセル	499
[Topology]ページでの関連するバックアップとクローンの表示	500
PowerShellコマンドレットを使用したセカンダリ バックアップ数のクリーンアップ	502
Windowsファイルシステムのリストア	503
Windowsファイルシステムのバックアップのリストア	503
PowerShellコマンドレットを使用したリソースのリストア	508
リストア処理の監視	511
リストア処理のキャンセル	512
Windowsファイルシステムのクローニング	513
Windowsファイルシステムのバックアップからのクローニング	513

クローニング処理の監視	519
クローニング処理のキャンセル	520
クローンのスプリット	521
Microsoft Exchange Serverデータベースの保護	523
SnapCenter Plug-in for Microsoft Exchange Serverの概念	523
SnapCenter Plug-in for Microsoft Exchange Serverの概要	523
SnapCenter Plug-in for Microsoft Exchange Serverの機能	523
SnapCenter Plug-in for Microsoft WindowsおよびSnapCenter Plug-in for Microsoft Exchange Serverでサポートされるストレージ タイプ	524
Exchangeプラグインに必要な最小ONTAP権限	525
SnapMirrorレプリケーションとSnapVaultレプリケーションのためのストレージ システムの準備	528
Exchange Serverリソースのバックアップ戦略の定義	528
Exchangeデータベースのリストア戦略の定義	531
SnapCenter Plug-in for Microsoft Exchange Serverのインストール	532
SnapCenter Plug-in for Microsoft Exchange Serverのインストール ワークフロー	532
ホストを追加してSnapCenter Plug-in for Microsoft Exchange Serverをインストールするための前提条件	533
SnapCenter Plug-in for Windowsのクレデンシャルの設定	537
Windows Server 2016以降でのgMSAの設定	538
ホストの追加とPlug-in for Exchangeのインストール	540
PowerShellコマンドレットを使用したSnapCenter ServerホストからのPlug-in for Exchangeのインストール	545
コマンドラインからのSnapCenter Plug-in for Exchangeのサイレント インストール	546
SnapCenterプラグイン パッケージのインストール ステータスの監視	547
CA証明書の設定	548
SnapManager 7.x for ExchangeとSnapCenterの共存の設定	551
SnapCenter Plug-in for VMware vSphereのインストール	553
CA証明書を導入する	553
CRLファイルを設定する	553
データ保護の準備	554
SnapCenter Plug-in for Microsoft Exchange Serverを使用するための前提条件	554
Exchange Serverの保護におけるソース、リソース グループ、ポリシーの使用方法	555
Exchangeリソースのバックアップ	556
バックアップのワークフロー	556
Exchangeのデータベースとバックアップの検証	557
Exchangeのリソースをバックアップに使用できるかどうかの確認	557
Exchange Serverデータベースのバックアップ ポリシーの作成	559
Exchange Serverのリソース グループの作成とポリシーの適用	566
Exchange Server用のPowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成	568
Exchangeデータベースのバックアップ	569

Exchangeリソース グループのバックアップ	575
バックアップ処理の監視	576
Exchangeデータベースのバックアップ処理のキャンセル	577
[Topology]ページでのExchangeバックアップの表示	578
Exchangeリソースのリストア	580
リストアのワークフロー	580
Exchangeデータベースをリストアする際の要件	580
Exchangeデータベースのリストア	581
メールとメールボックスのきめ細かなリカバリ	585
セカンダリ ストレージからのExchange Serverデータベースのリストア	585
Exchangeのパッシブ ノード レプリカの再シード	586
Exchangeデータベース用のPowerShellコマンドレットを使用したレプリカの再シード	586
リストア処理の監視	587
Exchangeデータベースのリストア処理のキャンセル	588
IBM Db2の保護	590
SnapCenter Plug-in for IBM Db2	590
SnapCenter Plug-in for IBM Db2の概要	590
SnapCenter Plug-in for IBM Db2の機能	590
SnapCenter Plug-in for IBM Db2の特長	591
SnapCenter Plug-in for IBM Db2でサポートされるストレージ タイプ	591
IBM Db2プラグインに必要な最小ONTAP権限	592
IBM Db2でのSnapMirrorレプリケーションとSnapVaultレプリケーションのためのストレージ システムの準備	595
IBM Db2のバックアップ戦略	595
IBM Db2のリストアとリカバリの戦略	598
SnapCenter Plug-in for IBM Db2のインストール準備	599
SnapCenter Plug-in for IBM Db2のインストール ワークフロー	599
Windows、Linux、またはAIX 用のホストを追加し、プラグイン パッケージをインストールするための前提条件	599
SnapCenter Plug-ins Package for Windowsをインストールするホストの要件	605
SnapCenter Plug-ins Package for Linuxをインストールするホストの要件	605
SnapCenter Plug-in for IBM Db2のクレデンシャルの設定	606
Windows Server 2016以降でのgMSAの設定	608
SnapCenter Plug-in for IBM Db2のインストール	609
CA証明書の設定	616
データ保護の準備	624
SnapCenter Plug-in for IBM Db2を使用するための前提条件	624
IBM Db2の保護におけるリソース、リソース グループ、ポリシーの使用法	624
IBM Db2リソースのバックアップ	625
IBM Db2リソースのバックアップ	625
データベースの自動的検出	627

手動でのプラグイン ホストへのリソースの追加	627
IBM Db2のバックアップ ポリシーの作成	629
リソース グループの作成とポリシーの適用	631
リソース グループを作成し、ASA r2 システム上の IBM Db2 リソースの二次保護を有効にします。	635
IBM Db2用のPowerShellコマンドレットを使用したストレージ	
システム接続とクレデンシャルの作成	637
Db2 データベースをバックアップする	639
リソース グループのバックアップ	646
IBM Db2バックアップ処理の監視	647
IBM Db2のバックアップ処理のキャンセル	648
[Topology]ページでのIBM Db2のバックアップとクローンの表示	649
IBM Db2のリストア	651
リストアのワークフロー	651
手動で追加されたリソース バックアップのリストア	651
自動検出されたデータベース バックアップのリストアとリカバリ	656
IBM Db2リストア処理の監視	658
IBM Db2リソースのバックアップのクローニング	658
クローニングのワークフロー	659
IBM Db2バックアップのクローニング	659
IBM Db2のクローニング処理の監視	666
クローンのスプリット	667
SnapCenterアップグレード後のIBM Db2データベースのクローンの削除またはスプリット	668
PostgreSQLの保護	670
SnapCenter Plug-in for PostgreSQL	670
SnapCenter Plug-in for PostgreSQLの概要	670
SnapCenter Plug-in for PostgreSQLの機能	670
SnapCenter Plug-in for PostgreSQLの特長	670
SnapCenter Plug-in for PostgreSQLでサポートされるストレージ タイプ	671
PostgreSQLプラグインに必要な最小ONTAP権限	672
PostgreSQLでのSnapMirrorレプリケーションとSnapVaultレプリケーションのためのストレージ	675
システムの準備	
PostgreSQLのバックアップ戦略	675
PostgreSQLのリストアとリカバリの戦略	678
SnapCenter Plug-in for PostgreSQLのインストール準備	679
SnapCenter Plug-in for PostgreSQLのインストール ワークフロー	679
ホストを追加してSnapCenter Plug-in for PostgreSQLをインストールするための前提条件	680
SnapCenter Plug-ins Package for Windowsをインストールするホストの要件	683
SnapCenter Plug-ins Package for Linuxをインストールするホストの要件	684
SnapCenter Plug-in for PostgreSQLのクレデンシャルの設定	685
Windows Server 2016以降でのgMSAの設定	687
SnapCenter Plug-in for PostgreSQLのインストール	688

CA証明書の設定	694
データ保護の準備	702
SnapCenter Plug-in for PostgreSQLを使用するための前提条件	702
PostgreSQLの保護におけるソース、リソース グループ、ポリシーの使用方法	703
PostgreSQL リソースのバックアップ	703
PostgreSQL リソースのバックアップ	703
クラスタの自動的検出	705
手動でのプラグイン ホストへのリソースの追加	705
PostgreSQLのバックアップ ポリシーの作成	707
リソース グループの作成とポリシーの適用	710
ASA r2 システム上の PostgreSQL リソースのリソース グループを作成し、二次保護を有効にする	714
PostgreSQL用のPowerShellコマンドレットを使用したストレージ	717
システム接続とクレデンシャルの作成	
PostgreSQLのバックアップ	718
リソース グループのバックアップ	724
PostgreSQLのバックアップ処理の監視	725
PostgreSQLのバックアップ処理のキャンセル	726
[Topology]ページでのPostgreSQLのバックアップとクローンの表示	727
PostgreSQLのリストア	729
リストアのワークフロー	729
手動で追加されたリソース バックアップのリストアとリカバリ	729
自動検出されたクラスタ バックアップのリストアとリカバリ	733
PowerShellコマンドレットを使用したリソースのリストア	736
PostgreSQLのリストア処理の監視	738
PostgreSQL リソースのバックアップのクローニング	739
クローニングのワークフロー	739
PostgreSQLのバックアップのクローニング	740
PostgreSQLのクローン処理の監視	743
クローンのスプリット	744
SnapCenterアップグレード後のPostgreSQLクラスタのクローンの削除またはスプリット	745
MySQLの保護	747
SnapCenter Plug-in for MySQL	747
SnapCenter Plug-in for MySQLの概要	747
SnapCenter Plug-in for MySQLの機能	747
SnapCenter Plug-in for MySQLの特長	747
SnapCenter Plug-in for MySQLでサポートされるストレージ タイプ	748
MySQLプラグインに必要な最小ONTAP権限	749
MySQLでのSnapMirrorレプリケーションとSnapVaultレプリケーションのためのストレージ	
システムの準備	752
MySQLのバックアップ戦略	752
MySQLのリストアとリカバリ戦略	755

SnapCenter Plug-in for MySQLのインストール準備	756
SnapCenter Plug-in for MySQLのインストール ワークフロー	756
ホストを追加してSnapCenter Plug-in for MySQLをインストールするための前提条件	756
SnapCenter Plug-ins Package for Windowsをインストールするホストの要件	760
SnapCenter Plug-ins Package for Linuxをインストールするホストの要件	761
SnapCenter Plug-in for MySQLのクレデンシャルの設定	762
SnapCenter Plug-in for MySQLのインストール	764
CA証明書の設定	769
データ保護の準備	777
SnapCenter Plug-in for MySQLを使用するための前提条件	777
MySQLの保護におけるソース、リソース グループ、ポリシーの使用方法	778
MySQLリソースのバックアップ	778
MySQLリソースのバックアップ	778
データベースの自動的検出	780
手動でのプラグイン ホストへのリソースの追加	780
MySQLのバックアップ ポリシーの作成	782
リソース グループの作成とポリシーの適用	785
リソース グループを作成し、ASA r2 システム上の MySQL リソースの二次保護を有効にする	789
MySQL用のPowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成	792
MySQLのバックアップ	793
リソース グループのバックアップ	799
MySQLのバックアップ処理の監視	800
MySQLのバックアップ処理のキャンセル	801
[Topology]ページでのMySQLのバックアップとクローンの表示	802
MySQLのリストア	804
リストアのワークフロー	804
手動で追加されたリソース バックアップのリストアとリカバリ	804
自動検出されたデータベース バックアップのリストアとリカバリ	808
PowerShellコマンドレットを使用したリソースのリストア	810
MySQLのリストア処理の監視	812
MySQLリソースのバックアップをクローニング	813
クローニングのワークフロー	813
MySQLバックアップのクローニング	814
MySQLのクローン処理の監視	817
クローンのスプリット	818
SnapCenterアップグレード後のMySQLデータベースのクローンの削除またはスプリット	819
NetAppがサポートするプラグインを使用してアプリケーションを保護する	821
NetAppがサポートしているプラグイン	821
NetAppがサポートしているプラグインの概要	821
NetAppがサポートしているプラグインの機能	821
NetAppがサポートしているプラグインの特長	822

NetAppがサポートしているプラグインでサポートされるストレージ タイプ	823
NetAppがサポートしているプラグインに必要な最小ONTAP権限	823
NetAppがサポートしているプラグインでSnapMirrorおよび SnapVaultレプリケーションを使うためのストレージ システムの準備	826
バックアップ戦略の定義	826
NetAppがサポートしているプラグインのバックアップ戦略	827
手動で追加したNetAppがサポートしているプラグイン リソースでサポートされるリストア戦略のタイプ	828
NetAppがサポートしているプラグインのインストール準備	828
SnapCenter NetAppがサポートしているプラグインのインストール ワークフロー	828
Windows、Linux、または AIX 用のホストを追加し、プラグイン パッケージをインストールするための前提条件	829
SnapCenter Plug-ins Package for Windowsをインストールするホストの要件	833
LinuxおよびAIX用のSnapCenterプラグインパッケージをインストールするためのホスト要件	834
NetAppがサポートしているプラグインのクレデンシャルの設定	835
Windows Server 2016以降でのgMSAの設定	837
NetAppがサポートしているプラグインのインストール	838
CA証明書の設定	845
データ保護の準備	853
NetAppがサポートしているプラグインを使用するための前提条件	853
NetAppがサポートしているプラグイン リソースの保護におけるリソース、リソース グループ、ポリシーの使用法	853
NetAppがサポートしているプラグイン リソースのバックアップ	854
NetAppがサポートしているプラグイン リソースのバックアップ	854
NetAppがサポートしているプラグインへのリソースの追加	855
NetAppがサポートしているプラグイン リソースのポリシーの作成	859
リソース グループの作成とポリシーの適用	863
リソース グループを作成し、ASA r2 システム上のリソースの二次保護を有効にします。	867
PowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成	869
NetAppがサポートしている個々のプラグイン リソースのバックアップ	870
NetAppがサポートしているプラグイン リソースのリソース グループのバックアップ	876
NetAppがサポートしているプラグインでのリソースのバックアップ処理の監視	877
NetAppがサポートしているプラグインのバックアップ処理のキャンセル	878
[Topology]ページでのNetAppがサポートしているプラグイン リソースに関連するバックアップとクローンの表示	879
NetAppがサポートしているプラグイン リソースのリストア	881
NetAppがサポートしているプラグイン リソースのリストア	881
リソースのバックアップのリストア	881
NetAppがサポートしているプラグインでのリソースのリストア処理の監視	885
NetAppがサポートしているプラグイン リソースのバックアップのクローニング	886
NetAppがサポートしているプラグイン リソースのバックアップのクローニング	886
バックアップからのクローニング	887

NetAppがサポートしているプラグインでのリソースのクローニング処理の監視	893
UNIXファイルシステムの保護	895
SnapCenter Plug-in for UNIX File Systemsの機能	895
サポートされている構成	895
制限事項	896
機能	896
SnapCenter Plug-in for UNIX File Systemsのインストール	896
ホストを追加してPlug-in Package for Linuxをインストールするための前提条件	896
GUIを使用したホストの追加とPlug-ins Package for Linuxのインストール	898
SnapCenter Plug-in Loaderサービスの設定	901
LinuxホストでのSnapCenter Plug-in Loader (SPL) サービスを使用したCA証明書の設定	904
プラグインのCA証明書の有効化	907
SnapCenter Plug-in for VMware vSphereのインストール	908
CA証明書を導入する	908
CRLファイルを設定する	908
UNIXファイルシステムの保護の準備	908
UNIXファイルシステムのバックアップ	909
バックアップに使用できるUNIXファイルシステムの検出	909
UNIXファイルシステムのバックアップ ポリシーの作成	909
UNIXファイルシステムのリソース グループの作成とポリシーの適用	912
ASA r2 システム上の Unix	914
ファイルシステムのリソースグループを作成し、二次保護を有効にします。	
UNIXファイルシステムのバックアップ	916
UNIXファイルシステム リソース グループのバックアップ	918
UNIXファイルシステムのバックアップの監視	918
[Topology]ページで保護されているUNIXファイルシステムの表示	920
UNIXファイルシステムのリストアとリカバリ	922
UNIXファイルシステムのリストア	922
UNIXファイルシステムのリストア処理の監視	923
UNIXファイルシステムのクローニング	924
UNIXファイルシステムのバックアップのクローニング	924
クローンのスプリット	926
UNIXファイルシステムのクローニング処理の監視	927
Azure NetApp Filesで実行されているアプリケーションの保護	929
Azure NetApp Filesで実行されているアプリケーションの保護	929
制限事項	929
SnapCenterのインストールとクレデンシャルの作成	929
Azure仮想マシンへのSnapCenterのインストール	929
SnapCenterでのAzureクレデンシャルの作成	931
Azureストレージ アカウントの設定	932
プラグイン ホストに追加するクレデンシャルの作成	932

SAP HANAデータベースの保護	933
ホストの追加とSnapCenter Plug-in for SAP HANA Databaseのインストール	933
SAP HANAデータベースの追加	934
SAP HANAデータベースのバックアップ ポリシーの作成	935
リソース グループの作成とSAP HANAバックアップ ポリシーの適用	935
Azure NetApp Filesで実行されているSAP HANAデータベースのバックアップ	936
SAP HANAリソース グループのバックアップ	937
SAP HANAデータベースのリストアとリカバリ	938
SAP HANAデータベースのバックアップのクローニング	939
Microsoft SQL Serverデータベースの保護	940
ホストの追加とSnapCenter Plug-in for SQL Server Databaseのインストール	940
SQL Serverデータベースのバックアップ ポリシーの作成	941
リソース グループの作成とSQLバックアップ ポリシーの適用	942
Azure NetApp Filesで実行されているSQL Serverデータベースのバックアップ	943
SQL Serverリソース グループのバックアップ	944
SQL Serverデータベースのリストアとリカバリ	945
SQL Serverデータベースのバックアップのクローニング	946
Oracleデータベースの保護	948
ホストの追加とSnapCenter Plug-in for Oracle Databaseのインストール	948
Oracleデータベースのバックアップ ポリシーの作成	948
リソース グループの作成とOracleバックアップ ポリシーの適用	949
Azure NetApp Filesで実行されているOracleデータベースのバックアップ	950
Oracleリソース グループのバックアップ	951
Oracleデータベースのリストアとリカバリ	952
Oracleデータベースのバックアップのクローニング	954
SnapCenter Serverとプラグインの管理	957
ダッシュボードの表示	957
ダッシュボードの概要	957
ダッシュボードに情報を表示する方法	961
ダッシュボードからのジョブ ステータス レポートのリクエスト	961
ダッシュボードからの保護ステータス レポートのリクエスト	962
RBACの管理	962
ロールの変更	962
ユーザとグループの変更	963
ホストの管理	963
仮想マシン情報の更新	965
プラグイン ホストの変更	966
プラグイン サービスの起動と再起動	967
ホスト メンテナンスのスケジュールの中断	967
[Resources]ページでサポートされる処理	968
ポリシーの管理	969

ポリシーの変更	969
ポリシーの適用解除	970
ポリシーの削除	970
リソース グループの管理	970
リソース グループに対する処理の停止および再開	971
リソース グループの削除	971
バックアップの管理	972
バックアップの名前の変更	972
バックアップの削除	972
保護の解除	973
クローンの削除	973
ジョブ、スケジュール、イベント、およびログの監視	974
ジョブの監視	974
スケジュールの監視	976
イベントを監視する	976
ログの監視	976
SnapCenterからのジョブとログの削除	977
SnapCenterのレポート機能の概要	978
レポートへのアクセス	979
レポートのフィルタ	980
レポートのエクスポートまたは印刷	980
Eメール通知用のSMTPサーバの設定	980
レポートのEメール送信オプションの設定	981
SnapCenter Serverリポジトリの管理	981
SnapCenterリポジトリを保護するための前提条件	981
SnapCenterリポジトリのバックアップ	982
SnapCenterリポジトリのバックアップの表示	982
SnapCenterデータベース リポジトリのリストア	982
SnapCenterリポジトリの移行	983
SnapCenterリポジトリのパスワードのリセット	984
信頼されていないドメインのリソースの管理	984
信頼されていないドメインの変更	985
信頼されていないActive Directoryドメインの登録解除	985
ストレージ システムの管理	986
ストレージ システムの設定の変更	986
ストレージ システムの削除	988
REST APIサポート	989
EMSデータ収集の管理	989
EMSデータ収集の停止	990
EMSデータ収集の開始	990
EMSデータ収集のスケジュールとターゲットSVMの変更	990

EMSデータ収集のステータス監視	990
SnapCenter Serverとプラグインのアップグレード	992
利用可能なアップデートを確認するためのSnapCenterの設定	992
アップグレード ワークフロー	992
サポートされているアップグレード パス	992
WindowsホストでのSnapCenter Serverのアップグレード	993
LinuxホストでのSnapCenter Serverのアップグレード	995
プラグイン パッケージのアップグレード	996
機器更改	999
SnapCenter Serverホストの機器更改	999
F5クラスタ内のノードの機器更改	1000
古いSnapCenter Serverホストの運用停止	1000
古いSnapCenter Serverホストへのロールバック	1000
ディザスタ リカバリ	1000
SnapCenterプラグイン ホストの機器更改	1002
ストレージ システムの機器更改	1005
プライマリ ストレージのバックアップの更新	1005
セカンダリ ストレージのバックアップの更新	1007
SnapCenter Serverとプラグインのアンインストール	1009
SnapCenterプラグイン パッケージのアンインストール	1009
ホストを削除するための前提条件	1009
ホストを削除する	1010
SnapCenter GUIを使用したプラグインのアンインストール	1011
PowerShellコマンドレットを使用したWindowsプラグインのアンインストール	1012
ホストでのプラグインのローカル アンインストール	1012
CLIを使用したPlug-ins Package for LinuxまたはPlug-ins Package for AIXのアンインストール	1013
WindowsホストでのSnapCenter Serverのアンインストール	1013
LinuxホストでのSnapCenter Serverのアンインストール	1014
REST APIを使用したSnapCenterの自動化	1015
REST APIを使用したSnapCenterの自動化	1015
SnapCenter REST APIヘネイティブにアクセスする方法	1015
基盤としてのREST Webサービス	1015
リソースと状態の表示	1015
URIエンドポイント	1016
HTTPメッセージ	1016
JSONの形式	1016
基本的な動作の特性	1016
要求と応答のAPIトランザクション	1016
CRUD操作のサポート	1016
オブジェクトID	1017
オブジェクトのインスタンスとコレクション	1017

同期操作と非同期操作	1017
セキュリティ	1017
API要求を制御する入力変数	1018
HTTPメソッド	1018
要求ヘッダー	1018
リクエスト本文	1019
オブジェクトのフィルタ	1019
特定のオブジェクト フィールドの要求	1019
出力セット内のオブジェクトのソート	1020
オブジェクトのコレクションを取得するときのページ付け	1020
サイズのプロパティ	1021
API応答の解釈	1021
HTTPステータス コード	1021
応答ヘッダー	1022
応答の本文	1022
エラー	1023
SnapCenter ServerとプラグインでサポートされているREST API	1024
認証	1024
ドメイン	1024
ジョブ	1024
設定	1024
ホスト	1025
リソース	1025
バックアップ	1027
クローン	1027
クローン スプリット	1028
リソース グループ	1028
ポリシー	1028
ストレージ	1029
共有	1029
プラグイン	1029
レポート	1030
アラート	1030
RBAC	1031
構成	1031
証明書設定	1031
リポジトリ	1031
version	1031
Swagger API WebページからREST APIにアクセスする方法	1032
REST APIの使用の開始	1032
Hello world	1032

法律上の表示	1034
著作権	1034
商標	1034
特許	1034
プライバシー ポリシー	1034
オープンソース	1034

SnapCenter software ドキュメント

リリース ノート

リリース ノート

SnapCenter 6.1 で利用できる新機能と強化された機能について説明します。

新機能と拡張機能の完全なリストについては、こちらをご覧ください。 ["SnapCenter 6.1の新機能"](#)。

既知の問題、制限事項、修正された問題、新規および変更されたコマンドの詳細については、 ["SnapCenterソフトウェア 6.1 リリースノート"](#)。リリース ノートにアクセスするには、NetAppアカウントでサインインするか、アカウントを作成する必要があります。

SnapCenterでサポートされているアップグレード パス

アップグレード パスは、以前のすべてのバージョンのSnapCenterから最新バージョンのSnapCenterにアップグレードできるかどうか、およびサポートされているプラグインのバージョンを把握するのに役立ちます。

SnapCenter Serverのバージョン	SnapCenter Serverを直接アップグレードできる環境	サポートされているプラグインのバージョン
5.0	6.0	• 5.0 • 6.0
	6.0.1	• 6.0.1
	6.1	• 6.1
6.0	6.0.1	• 6.0 • 6.0.1
	6.1	• 6.1
6.0.1	6.1	• 6.0.1 • 6.1

SnapCenter Plug-in for VMware vSphere のアップグレードについては、以下を参照してください。 ["SnapCenter Plug-in for VMware vSphereのアップグレード"](#)。

始めましょう

SnapCenter softwareについて学ぶ

SnapCenterの概要

SnapCenter softwareは、アプリケーション一貫性のあるデータ保護を実現するシンプルで集中化されたスケーラブルなプラットフォームです。ハイブリッド クラウド内のONTAPシステム上のアプリケーション、データベース、ホスト ファイル システム、および VM を保護します。

SnapCenter は、NetApp Snapshot、SnapRestore、FlexClone、SnapMirror、およびSnapVaultテクノロジーを使用して、次の機能を提供します。

- 高速でスペース効率に優れ、アプリケーションと整合性のあるディスクベースのバックアップ
- 高速で詳細なリストアとアプリケーション整合性のあるリカバリ
- スペース効率に優れた迅速なクローニング

SnapCenterには、SnapCenter Server と軽量プラグインが含まれています。リモート アプリケーション ホストへのプラグインの展開を自動化し、バックアップ、検証、クローン操作をスケジュールし、データ保護操作を監視することができます。

データを保護するために、SnapCenter をオンプレミスまたはパブリック クラウドにインストールできます。

- オンプレミスでは次のものを保護します。
 - ONTAP FAS、AFF、またはASAプライマリ システム上にあり、ONTAP FAS、AFF、またはASAセカンダリ システムに複製されたデータ
 - ONTAP Selectプライマリ システム上のデータ
 - ONTAP FAS、AFF、またはASAのプライマリ システムとセカンダリ システム上にあり、ローカルのStorageGRIDオブジェクト ストレージに保護されているデータ
 - ONTAP ASA r2プライマリおよびセカンダリシステムにあるデータ
- ハイブリッド クラウド内のオンプレミスで次のものを保護します。
 - ONTAP FAS、AFF、またはASAのプライマリ システム上にあり、Cloud Volumes ONTAPにレプリケートされているデータ
 - ONTAP FAS、AFF、またはASAのプライマリ システムとセカンダリ システム上にあり、クラウドのオブジェクト ストレージとアーカイブ ストレージに保護されているデータ（BlueXPバックアップとリカバリの統合を使用）
- パブリック クラウドに導入（以下のデータを保護）：
 - Cloud Volumes ONTAP（旧称ONTAP Cloud）プライマリ システム上のデータ
 - Amazon FSX for ONTAP上のデータ
 - プライマリAzure NetApp Files（Oracle、Microsoft SQL、SAP HANA）上のデータ

主な機能

SnapCenter は次の主な機能を提供します。

- さまざまなアプリケーションの集中型でアプリケーション一貫性のあるデータ保護

データ保護は、Microsoft Exchange Server、Microsoft SQL Server、Linux または AIX 上の Oracle データベース、SAP HANA データベース、IBM Db2、PostgreSQL、MySQL、および ONTAP システムで実行されている Windows ホスト ファイル システムでサポートされています。SnapCenter は、MongoDB、Storage、MaxDB、Sybase ASE、ORASCPM などのアプリケーションの保護もサポートしています。

- ポリシーベースのバックアップ

ポリシーベースのバックアップでは、NetApp Snapshot テクノLOGY を利用して、高速でスペース効率に優れ、アプリケーションと整合性のあるディスクベースのバックアップを作成します。既存の保護関係を更新することで、これらのバックアップをセカンダリ ストレージに自動的に保護するように設定することもできます。

- 複数のリソースのバックアップ

SnapCenter リソース グループを使用すると、同じ種類の複数のリソース (アプリケーション、データベース、またはホスト ファイル システム) を一度にバックアップできます。

- リストアとリカバリ

SnapCenter は、バックアップの迅速できめ細かなリストアと、アプリケーションと整合性のある時間ベースのリカバリを実現します。リストアは、ハイブリッド クラウド内の任意のデスティネーションから実行できます。

- クローニング

SnapCenter は、迅速でスペース効率が高く、アプリケーションと一貫性のあるクローン作成を実現します。クローニングは、ハイブリッド クラウド内の任意のデスティネーションで実行できます。

- 単一ユーザー管理グラフィカルユーザーインターフェース

SnapCenter は、あらゆるハイブリッド クラウドの宛先のバックアップとクローンを管理するための単一のインターフェースを提供します。

- REST API、Windows コマンドレット、UNIX コマンド

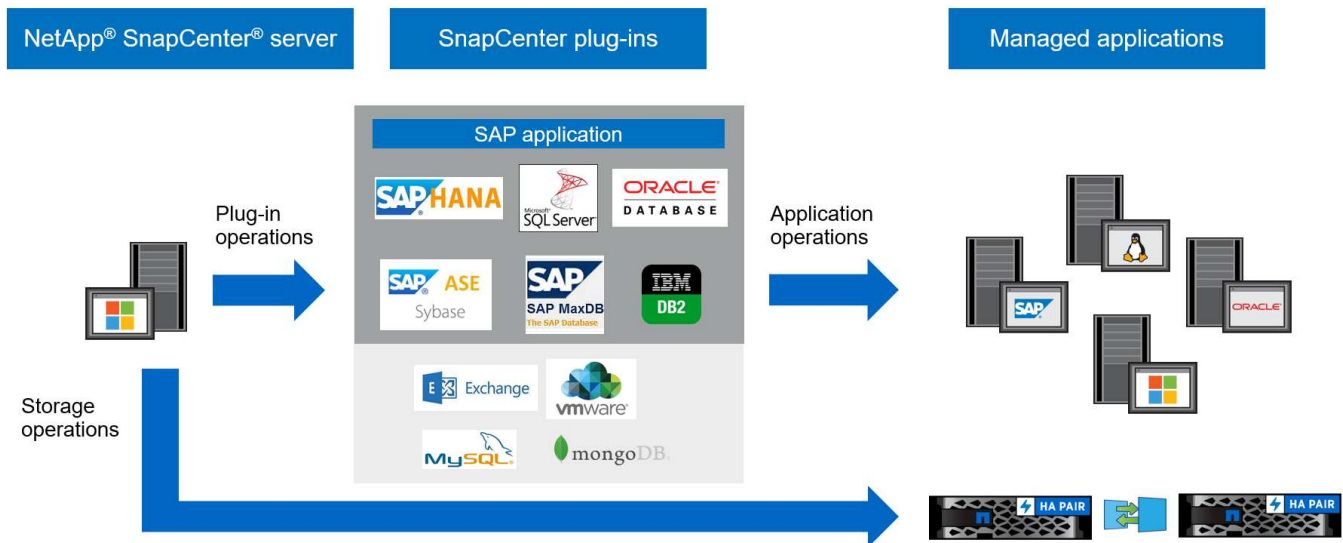
SnapCenter は、あらゆるオーケストレーション ソフトウェアとの統合、および Windows PowerShell コマンドレットとコマンド ライン インターフェースの使用のためのほとんどの機能に対して REST API を提供します。

- 一元化されたデータ保護ダッシュボードとレポート
- セキュリティと委任のためのロールベースアクセス制御 (RBAC)
- すべてのバックアップメタデータを保存するための高可用性を備えた組み込みリポジトリデータベース
- プラグインのプッシュ インストールの自動化
- 高可用性
- ディザスタ リカバリ (DR)

- SnapLock ["詳細情報"](#)
- SnapMirrorアクティブ シンク (当初はSnapMirror Business Continuity [SM-BC] としてリリース)
- 同期ミラーリング ["詳細情報"](#)

SnapCenterのアーキテクチャとコンポーネント

SnapCenter は、中央管理サーバーとプラグイン ホストを使用した階層化設計を使用します。サーバーとプラグイン ホストは異なる場所に配置できます。



SnapCenterには、 SnapCenter Server、Windows 用のSnapCenterプラグイン パッケージ、Linux 用のSnapCenterプラグイン パッケージが含まれています。各パッケージには、さまざまなアプリケーションおよびインフラストラクチャ コンポーネント用のプラグインが含まれています。

SnapCenter Server

SnapCenter Server は、Microsoft Windows および Linux (RHEL 8.x、RHEL 9.x、SLES 15 SP5) オペレーティング システムをサポートしています。 SnapCenterサーバーには、Web サーバー、集中型の HTML5 ベースのユーザー インターフェイス、PowerShell コマンドレット、REST API、およびSnapCenterリポジトリが含まれています。

SnapCenter は、操作に関する情報をSnapCenterリポジトリに保存します。

SnapCenterプラグイン

各SnapCenterプラグインは、特定の環境、データベース、アプリケーションをサポートします。

プラグイン名	インストールパッケージ	他に必要なプラグイン	インストール先のホスト	サポートされているプラットフォーム
Microsoft SQL Server 用のSnapCenterプラグイン	Windows用プラグインパッケージ	Plug-in for Windows	SQL Serverホスト	Windows

プラグイン名	インストール パッケージ	他に必要なプラグイ ン	インストール先のホ スト	サポートされている プラットフォーム
Windows 用SnapCenterプラ グイン	Windows用プラグイ ンパッケージ		Windowsホスト	Windows
Microsoft Exchange Server 用 のSnapCenterプラ グイン	Windows用プラグイ ンパッケージ	Plug-in for Windows	Exchange Serverホ スト	Windows
Oracle データベース 用の SnapCentre プ ラグイン	Linux用プラグイン パッケージとAIX用 プラグインパッケー ジ	Plug-in for UNIX	Oracleホスト	LinuxまたはAIX
SAP HANA データ ベース用 のSnapCenterプラ グイン	Linux用プラグイン パッケージとWindows用プラグ インパッケージ	UNIX用プラグイン またはWindows用プ ラグイン	HDBSQLクライアン ト ホスト	Linuxまた はWindows
IBM Db2 用 のSnapCenterプラ グイン	Linux用プラグイン パッケージとWindows用プラグ インパッケージ	UNIX用プラグイン またはWindows用プ ラグイン	Db2ホスト	Linux、AIX、 また はWindows
PostgreSQL 用SnapCenterプラ グイン	Linux用プラグイン パッケージとWindows用プラグ インパッケージ	UNIX用プラグイン またはWindows用プ ラグイン	PostgreSQLホスト	Linuxまた はWindows
MySQL 用SnaoCenterプラ グイン	Linux用プラグイン パッケージとWindows用プラグ インパッケージ	Plug-in for UNIXまた はPlug-in for Windows	MySQLホスト	Linuxまた はWindows
MongoDB 用 のSnapCenterプラ グイン	Linux用プラグイン パッケージとWindows用プラグ インパッケージ	UNIX用プラグイン またはWindows用プ ラグイン	MongoDBホスト	Linuxまた はWindows
ORASCPM 用SnapCenterプラ グイン (Oracle アプ リケーション)	Linux用プラグイン パッケージとWindows用プラグ インパッケージ	UNIX用プラグイン またはWindows用プ ラグイン	Oracleホスト	Linuxまた はWindows

プラグイン名	インストールパッケージ	他に必要なプラグイン	インストール先のホスト	サポートされているプラットフォーム
SAP ASE 用のSnapCenterプラグイン	Linux用プラグインパッケージとWindows用プラグインパッケージ	UNIX用プラグインまたはWindows用プラグイン	SAPホスト	LinuxまたはWindows
SAP MaxDB 用のSnapCenterプラグイン	Linux用プラグインパッケージとWindows用プラグインパッケージ	UNIX用プラグインまたはWindows用プラグイン	SAP MaxDBホスト	LinuxまたはWindows
ストレージプラグイン用のSnapCenterプラグイン	Linux用プラグインパッケージとWindows用プラグインパッケージ	UNIX用プラグインまたはWindows用プラグイン	ストレージホスト	LinuxまたはWindows

SnapCenter Plug-in for VMware vSphereは、仮想マシン (VM)、データストア、仮想マシン ディスク (VMDK) のクラッシュ整合性および VM 整合性のバックアップとリストア操作をサポートします。また、仮想化されたデータベースとファイル システムのアプリケーション整合性のあるバックアップおよび復元操作もサポートします。

データベース、ファイルシステム、VM、またはVM上のデータストアを保護するには、SnapCenter Plug-in for VMware vSphereを展開します。詳細については、["SnapCenter Plug-in for VMware vSphereのドキュメント"](#)。

SnapCenterリポジトリ

SnapCenterリポジトリ（NSMデータベースとも呼ばれる）には、SnapCenterのすべての処理についての情報とメタデータが保存されます。

SnapCenter Server をインストールすると、デフォルトで MySQL Server リポジトリ データベースがインストールされます。MySQL Server がすでにインストールされていて、SnapCenter Server の新規インストールを実行する場合は、MySQL Server をアンインストールする必要があります。

SnapCenterでは、SnapCenterリポジトリ データベースとしてMySQL Server 8.0.37以降がサポートされます。以前のバージョンのMySQL Server を以前のリリースのSnapCenterと併用する場合、SnapCenterのアップグレード プロセスによってMySQL Server はバージョン 8.0.37 以降にアップグレードされます。

SnapCenterリポジトリには、次の情報とメタデータが保存されます。

- バックアップ、クローン、リストア、検証のメタデータ
- レポート作成、ジョブ、イベントの情報
- ホストおよびプラグインの情報
- ロール、ユーザ、アクセス許可の詳細
- ストレージ システムの接続情報

SnapCenterのセキュリティ機能

SnapCenterでは、データの安全を確保するために厳格なセキュリティおよび認証機能を採用しています。

SnapCenterのセキュリティ機能を次に示します。

- SnapCenterへの通信には、いずれもHTTP over SSL (HTTPS) が使用されます。
- SnapCenterでは、すべてのクレデンシャルがAdvanced Encryption Standard (AES) 暗号化を使用して保護されます。
- 連邦情報処理標準 (FIPS) に準拠したセキュリティ アルゴリズムをサポートします。
- 顧客が提供する認定 CA 証明書の使用をサポートします。
- ONTAPとの通信に Transport Layer Security (TLS) 1.3 をサポートします。クライアントとサーバの間の通信にもTLS 1.2を使用できます。
- ネットワーク通信全体のセキュリティを確保するために、特定の SSL 暗号スイートのセットをサポートします。 ["詳細情報"](#)。
- SnapCenterは、会社のファイアウォールの内側にインストールされます。これにより、SnapCenter Serverへのアクセス、およびSnapCenter Serverとプラグインの間の通信が可能になります。
- SnapCenter APIおよび処理アクセスでは、AES暗号化で暗号化されたトークンが使用されます。このトークンは24時間後に期限切れになります。
- SnapCenterのログインは、Windows Active Directoryと統合されています。また、アクセス権限を制御するロールベース アクセス制御 (RBAC) も統合されています。
- IPsec は、Windows および Linux ホスト マシンのONTAP上のSnapCenterでサポートされています。 ["詳細情報"](#)。
- SnapCenterのPowerShellコマンドレット セッションはセキュリティで保護されます。
- デフォルトでは、操作を行わないまま15分が経過すると、5分後にSnapCenterからログアウトすることを示す警告が表示されます。

最後に操作を行ってから20分が経過した時点で、SnapCenterからログアウトされ、再ログインが必要になります。ログアウト期間は変更できます。

- 5 回連続してログインを間違えると、一時的にログインが無効になります。
- SnapCenter Server とONTAP間の CA 証明書認証をサポートします。 ["詳細情報"](#)。
- 整合性検証ツールがSnapCenter Serverとプラグインに追加され、新規インストールおよびアップグレード処理の際に、配布されたすべてのバイナリが検証されます。

CA証明書の概要

SnapCenter Serverインストーラでのインストール中、一元的なSSL証明書のサポートが有効になります。SnapCenterでは、サーバとプラグイン間のセキュアな通信を強化するために、お客様から提供された承認済みCA証明書の使用がサポートされています。

SnapCenter Server とそれぞれのプラグインをインストールした後、CA 証明書を展開する必要があります。詳細については、以下を参照してください。 ["CA証明書CSRファイルの生成"](#)。

SnapCenter Plug-in for VMware vSphereのCA証明書を導入することもできます。詳細については、以下を参照してください。"[証明書を作成とインポート](#)"。

双方向SSL通信

双方向SSL通信は、SnapCenter Serverとプラグインの間の相互通信を保護します。

証明書ベースの認証の概要

証明書ベースの認証によって、SnapCenterプラグイン ホストにアクセスしようとする各ユーザの真正性を検証します。ユーザは秘密キーなしでSnapCenter Server証明書をエクスポートし、プラグイン ホストの信頼されたストアにインポートする必要があります。証明書ベースの認証は、双方向SSL機能が有効になっている場合にのみ機能します。

多要素認証 (MFA)

MFAでは、Security Assertion Markup Language (SAML) を介してサードパーティのアイデンティティ プロバイダ (IdP) を使用して、ユーザ セッションを管理します。この機能は、既存のユーザ名とパスワードと併せて、TOTP、生体認証、プッシュ通知などの複数の要素を使用するオプションを提供することで、認証セキュリティを強化します。また、お客様は独自のユーザ アイデンティティ プロバイダを使用して、ポートフォリオ全体で統合ユーザ ログイン (SSO) を実現できます。

MFAは、SnapCenter Server UIログインにのみ適用されます。ログインはIdP Active Directory Federation Services (AD FS) を使用して認証されます。AD FSでは、さまざまな認証要素を設定できます。SnapCenterはサービス プロバイダであるため、AD FSでSnapCenterを証明書利用者として設定する必要があります。SnapCenterでMFAを有効にするには、AD FSメタデータが必要です。

MFAを有効にする方法については、以下を参照してください。"[多要素認証を有効にする](#)"。

SnapCenterのロールベースのアクセス制御

SnapCenterのロールベース アクセス制御 (RBAC) とONTAPの権限を使用すると、SnapCenter管理者は、SnapCenterリソースの制御を別のユーザまたはユーザ グループに委任できます。この方法でアクセスを一元管理することで、アプリケーション管理者がそれぞれの委譲された環境で安全に作業することができます。

いつでもロールを作成および変更し、ユーザーにリソース アクセスを追加できます。ただし、SnapCenterを初めてセットアップする場合は、少なくとも Active Directory ユーザーまたはグループをロールに追加し、それらのユーザーまたはグループにリソース アクセスを追加する必要があります。



SnapCenterを使用して、ユーザ アカウントやグループ アカウントを作成することはできません。ユーザ アカウントやグループ アカウントは、オペレーティング システムまたはデータベースのActive Directoryに作成する必要があります。

SnapCenterのRBACの種類

SnapCenterでは、次の種類のロールベース アクセス制御を使用します。

- SnapCenter RBAC
- アプリケーションレベルのRBAC

- VMware vSphere RBAC 用のSnapCenterプラグイン
- ONTAP権限

SnapCenter RBAC

SnapCenterには事前定義されたロールがあり、ユーザーまたはユーザー グループをこれらのロールに割り当てることができます。事前定義されたロールは次のとおりです。

- SnapCenter管理者ロール
- App Backup and Clone Adminロール
- Backup and Clone Viewerロール
- Infrastructure Adminロール

ユーザーにロールを割り当てると、SnapCenterAdmin ロールを割り当てていない限り、そのユーザーに関連するジョブのみが [ジョブ] ページに表示されます。

また、新しいロールを作成して権限とユーザを管理することもできます。ホスト、ストレージ接続、リソースグループなどのSnapCenterオブジェクトにアクセスするための権限をユーザまたはグループに割り当てることができます。

RBACの権限は、同じフォレスト内のユーザとグループ、および別のフォレストに属しているユーザに割り当てることができます。フォレストにまたがってネストされたグループに属するユーザには、RBACの権限を割り当てることはできません。



カスタム ロールを作成する場合は、SnapCenterAdmin ロールのすべての権限を含める必要があります。「Host add」や「Host remove」など、一部の権限しかコピーしなかった場合、それらの処理を実行することはできません。

ユーザは、グラフィカル ユーザ インターフェイス (GUI) またはPowerShellコマンドレットを使用して、ログインする際に認証情報を指定する必要があります。ユーザが複数のロールに割り当てられている場合は、ログイン クレデンシャルの入力後に、使用するロールを指定するように求められます。また、APIを実行する際にも認証が必要になります。

アプリケーションレベルのRBAC

SnapCenterでは、クレデンシャルを使用して、権限のあるSnapCenterユーザにアプリケーションレベルの権限も付与されていることを検証します。

たとえば、SQL Server 環境でデータ保護操作を実行する場合は、適切な Windows または SQL 資格情報を使用して資格情報を設定する必要があります。SnapCenter Serverは、どちらの方法で設定されたクレデンシャルも認証します。ONTAPストレージ上の Windows ファイル システム環境でデータ保護操作を実行する場合、SnapCenter管理者ロールには Windows ホストに対する管理者権限が必要です。

同様に、Oracleデータベースに対してデータ保護処理を実行する場合、データベース ホストでオペレーティング システム (OS) 認証が無効なときは、クレデンシャルにOracleデータベースまたはOracle ASMのクレデンシャルを設定する必要があります。SnapCenter Serverは、処理に応じて、いずれかの方法で設定されたクレデンシャルを認証します。

SnapCenter Plug-in for VMware vSphereのRBAC

VMと整合性のあるデータ保護にSnapCenter VMwareプラグインを使用する場合は、vCenter ServerでRBACをさらに強化できます。SnapCenter VMware プラグインは、vCenter Server RBAC とONTAP RBAC の両方をサポートします。 ["詳細情報"](#)

ベスト プラクティス: NetApp、 SnapCenter Plug-in for VMware vSphere操作用に 1 つのONTAPロールを作成し、必要なすべての権限を割り当てることを推奨しています。

ONTAP権限

ストレージ システムにアクセスするために必要な権限を持つ vsadmin アカウントを作成する必要があります。 ["詳細情報"](#)

定義済みのSnapCenterロールに割り当てられた権限

ロールにユーザを追加するときは、Storage Connection権限を割り当ててStorage Virtual Machine (SVM) の通信を有効にするか、SVMをユーザに割り当ててそのSVMを使用する権限を有効にする必要があります。ストレージ接続権限により、ユーザーは SVM 接続を作成できます。

たとえば、SnapCenter管理者ロールを持つユーザーは SVM 接続を作成し、それを App Backup and Clone 管理者ロールを持つユーザーに割り当てることができます。このロールを持つユーザーには、デフォルトでは SVM 接続を作成または編集する権限がありません。SVM 接続がないと、ユーザーはバックアップ、クローン、または復元操作を完了できません。

SnapCenter管理者ロール

SnapCenter管理者ロールにはすべての権限が有効になっています。このロールの権限を変更することはできません。ロールに対しては、ユーザやグループを追加または削除できます。

App Backup and Clone Adminロール

App Backup and Clone Adminロールには、アプリケーション バックアップとクローン関連のタスクに対して管理操作を実行するために必要な権限が付与されています。ホスト管理、プロビジョニング、ストレージ接続管理、リモート インストールに必要な権限は含まれていません。

権限	有効	作成	読み取り	更新	削除
Resource Group	該当なし	はい	はい	はい	はい
ポリシー	該当なし	はい	はい	はい	はい
バックアップ	該当なし	はい	はい	はい	はい
ホスト	該当なし	はい	はい	はい	はい
ストレージ接続	該当なし	いいえ	はい	いいえ	いいえ
クローン	該当なし	はい	はい	はい	はい

権限	有効	作成	読み取り	更新	削除
Provision	該当なし	いいえ	はい	いいえ	いいえ
ダッシュボード	はい	該当なし	該当なし	該当なし	該当なし
レポート	はい	該当なし	該当なし	該当なし	該当なし
リストア	はい	該当なし	該当なし	該当なし	該当なし
リソース	はい	はい	はい	はい	はい
プラグインのインストール/アンインストール	いいえ	該当なし		該当なし	該当なし
移住	いいえ	該当なし	該当なし	該当なし	該当なし
マウント	はい	はい	該当なし	該当なし	該当なし
アンマウント	はい	はい	該当なし	該当なし	該当なし
Full Volume Restore	いいえ	いいえ	該当なし	該当なし	該当なし
二次保護	いいえ	いいえ	該当なし	該当なし	該当なし
ジョブモニター	はい	該当なし	該当なし	該当なし	該当なし

Backup and Clone Viewerロール

Backup and Clone Viewerロールには、すべての権限の読み取り専用権限が付与されています。また、検出、レポート、およびダッシュボードへのアクセスに必要な権限も有効になっています。

権限	有効	作成	読み取り	更新	削除
Resource Group	該当なし	いいえ	はい	いいえ	いいえ
ポリシー	該当なし	いいえ	はい	いいえ	いいえ
バックアップ	該当なし	いいえ	はい	いいえ	いいえ
ホスト	該当なし	いいえ	はい	いいえ	いいえ
ストレージ接続	該当なし	いいえ	はい	いいえ	いいえ

権限	有効	作成	読み取り	更新	削除
クローン	該当なし	いいえ	はい	いいえ	いいえ
Provision	該当なし	いいえ	はい	いいえ	いいえ
ダッシュボード	はい	該当なし	該当なし	該当なし	該当なし
レポート	はい	該当なし	該当なし	該当なし	該当なし
リストア	いいえ	いいえ	該当なし	該当なし	該当なし
リソース	いいえ	いいえ	はい	はい	いいえ
プラグインのインストール/アンインストール	いいえ	該当なし	該当なし	該当なし	該当なし
移住	いいえ	該当なし	該当なし	該当なし	該当なし
マウント	はい	該当なし	該当なし	該当なし	該当なし
アンマウント	はい	該当なし	該当なし	該当なし	該当なし
Full Volume Restore	いいえ	該当なし	該当なし	該当なし	該当なし
二次保護	いいえ	該当なし	該当なし	該当なし	該当なし
ジョブモニター	はい	該当なし	該当なし	該当なし	該当なし

Infrastructure Adminロール

Infrastructure Adminロールでは、ホストの管理、ストレージの管理、プロビジョニング、リソース グループ、リモート インストールのレポート、およびダッシュボードへのアクセスに必要な権限が有効になっています。

権限	有効	作成	読み取り	更新	削除
Resource Group	該当なし	はい	はい	はい	はい
ポリシー	該当なし	いいえ	はい	はい	はい
バックアップ	該当なし	はい	はい	はい	はい

権限	有効	作成	読み取り	更新	削除
ホスト	該当なし	はい	はい	はい	はい
ストレージ接続	該当なし	はい	はい	はい	はい
クローン	該当なし	いいえ	はい	いいえ	いいえ
Provision	該当なし	はい	はい	はい	はい
ダッシュボード	はい	該当なし	該当なし	該当なし	該当なし
レポート	はい	該当なし	該当なし	該当なし	該当なし
リストア	はい	該当なし	該当なし	該当なし	該当なし
リソース	はい	はい	はい	はい	はい
プラグインのインストール/アンインストール	はい	該当なし	該当なし	該当なし	該当なし
移住	いいえ	該当なし	該当なし	該当なし	該当なし
マウント	いいえ	該当なし	該当なし	該当なし	該当なし
アンマウント	いいえ	該当なし	該当なし	該当なし	該当なし
Full Volume Restore	いいえ	いいえ	該当なし	該当なし	該当なし
二次保護	いいえ	いいえ	該当なし	該当なし	該当なし
ジョブモニター	はい	該当なし	該当なし	該当なし	該当なし

SnapCenterでの災害復旧

SnapCenter の災害復旧 (DR) 機能を使用すると、リソースの破損やサーバーのクラッシュなどの災害から復旧できます。SnapCenterリポジトリ、サーバー スケジュール、構成コンポーネント、SQL Server 用のSnapCenterプラグインとそのストレージを復元するのに役立ちます。

このセクションでは、SnapCenterの 2 種類の DR について説明します。

SnapCenterサーバー DR

- SnapCenter Serverでプラグインの追加や管理をすることなくSnapCenter Serverのデータをバックアップし、リカバリできます。
- セカンダリSnapCenter Serverは、プライマリSnapCenter Serverと同じディレクトリ、同じポートにインストールする必要があります。
- 多要素認証 (MFA) の場合、SnapCenter Server DR 中にすべてのブラウザ タブを閉じ、ブラウザを再度開いて再度ログインします。これにより既存の、またはアクティブなセッションCookieがクリアされ、正しい設定データが更新されます。
- SnapCenter の災害復旧機能は、REST API を使用してSnapCenterサーバーをバックアップします。見る["SnapCenter Serverのディザスタ リカバリにおけるREST APIのワークフロー"](#)。
- 監査設定関連の構成ファイルは、DR バックアップにも、復元操作後の DR サーバーにもバックアップされません。監査ログの設定については、手動で再現する必要があります。

SnapCenterプラグインとストレージ DR

DR は、SQL Server 用のSnapCenterプラグインでのみ使用できます。プラグインがダウンしている場合は、別の SQL ホストに切り替えて、いくつかの手順に従ってデータを回復します。見る["SnapCenter Plug-in for SQL Serverのディザスタ リカバリ"](#)。

SnapCenter はONTAP SnapMirrorを使用してデータを複製します。これにより、セカンダリ サイトにデータを同期させておくことで DR に使用できます。フェイルオーバーを開始するには、SnapMirrorレプリケーションを中断します。フォールバック中は、同期を逆にして、DR サイトからプライマリ ロケーションにデータを複製します。

SnapCenterに必要なライセンス

SnapCenterでは、アプリケーション、データベース、ファイルシステム、仮想マシンのデータ保護を実現するために複数のライセンスが必要です。インストールするSnapCenterライセンスのタイプは、ストレージ環境および使用する機能によって異なります。

ライセンス	インストール先
SnapCenter Standard (コントローラ ベース)	FAS、AFF、ASAに必須 SnapCenter Standard ライセンスはコントローラ ベースのライセンスであり、NetApp ONTAP One の一部として含まれています。SnapManager Suiteライセンスには、SnapCenter Standardライセンスの使用権も付随しています。FAS、AFF、またはASAストレージを使用してSnapCenterを試用インストールする場合は、営業担当者に連絡してNetApp ONTAP One 評価ライセンスを入手できます。 NetApp ONTAP Oneに含まれるライセンスの詳細については、"NetApp ONTAP Oneに含まれるライセンス"。  SnapCenterは、Data Protection Bundleの一部としても提供されます。A400以降を購入済みの場合は、Data Protection Bundleを購入する必要があります。
SnapMirror / SnapVault	ONTAP SnapCenterでレプリケーションを有効にする場合、SnapMirrorまたはSnapVaultどちらかのライセンスが必要です。
SnapRestore	バックアップのリストアと検証に必要です。 プライマリ ストレージ システム • SnapVaultデスティネーション システムでリモート検証とバックアップからのリストアを実行するために必要です。 • SnapMirrorデスティネーション システムでリモート検証を実行するために必要です。

ライセンス	インストール先
FlexClone	データベースのクローニング処理と検証処理に必要です。 プライマリ ストレージ システムとセカンダリ ストレージ システム • SnapVaultデスティネーション システムでセカンダリ バックアップからクローンを作成するために必要です。 • SnapMirrorデスティネーション システムでセカンダリ SnapMirrorバックアップからクローンを作成するために必要です。
プロトコルライセンス	• LUN用のiSCSIライセンスまたはFCライセンス • SMB共有用のCIFSライセンス • NFSタイプのVMDK用のNFSライセンス • VMFSタイプのVMDK用のiSCSIライセンスまたはFCライセンス ソース ボリュームを利用できない場合にSnapMirrorデスティネーション システムからデータを提供するには、SnapMirrorデスティネーション システムに必要です。
SnapCenter Standardライセンス（オプション）	セカンダリ デスティネーション  セカンダリ デスティネーションにSnapCenter Standardライセンスを追加することを推奨しますが、必須ではありません。セカンダリ デスティネーションでSnapCenter Standardライセンスが有効になっていない場合、フェイルオーバー後にSnapCenterを使用してセカンダリ デスティネーションでリソースをバックアップすることができません。ただし、クローン処理と検証処理を実行するためには、セカンダリ デスティネーションにFlexCloneライセンスが必要です。

ライセンス	インストール先
Single Mailbox Recovery (SMBR) ライセンス	SnapCenter Plug-in for Exchangeを使用してMicrosoft Exchange ServerのデータベースとSingle Mailbox Recovery (SMBR) を管理する場合は、SMBR用の追加ライセンスが必要です。このライセンスはユーザのメールボックス数に基づいて別途購入する必要があります。 NetApp® Single Mailbox Recoveryは、2023年5月12日に販売終了（EOA）になりました。詳細については、"CPC-00507"。2020年6月24日に導入された販売用パーツ番号を通じてメールボックスの容量、メンテナンス、サポートを購入されたお客様には、サポート対象の期間中は引き続きサポートを提供いたします。 NetApp Single Mailbox Recoveryは、Ontrackが提供するパートナー製品です。Ontrack PowerControlsには、NetApp Single Mailbox Recoveryと同様の機能が用意されています。販売終了となる2023年5月12日以降、お客様は、新しいOntrack PowerControlsソフトウェア ライセンスとOntrack PowerControlsのメンテナンスおよびサポート更新をOntrackから（licensingteam@ontrack.com経由で）購入して、メールボックスをきめ細かくリカバリできます。



SnapCenter AdvancedとSnapCenter NAS File Servicesのライセンスは廃止され、現在は提供されていません。Amazon FSx for NetApp ONTAP、ONTAP Select、Cloud Volumes ONTAP、およびAzure NetApp Files、標準ライセンスと容量ベースのライセンスは不要になりました。

1つ以上のSnapCenterライセンスをインストールする必要があります。ライセンスの追加方法については、以下を参照してください。"[SnapCenter Standardコントローラベース ライセンスの追加](#)"。

SnapCenterのSnapMirrorアクティブ同期

SnapMirrorアクティブ同期を使用すると、サイト全体の障害が発生した場合でもビジネス サービスの運用を継続でき、アプリケーションがセカンダリ コピーを使用して透過的にフェイルオーバーできるようになります。SnapMirrorアクティブ同期でフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。

SnapMirrorアクティブ同期の詳細については、以下を参照してください。"[SnapMirrorアクティブ同期の概要](#)"。

SnapMirrorアクティブ同期を使用するために、ハードウェア、ソフトウェア、およびシステムのさまざまな設定要件を満たしていることを確認します。詳細については、"[前提条件](#)"

この機能でサポートされるプラグインは、SnapCenter Plug-in for SQL Server、SnapCenter Plug-in for Windows、SnapCenter Plug-in for Oracleデータベース、SnapCenter Plug-in for SAP HANAデータベース、SnapCenter Plug-in for Microsoft Exchange Server、SnapCenter Plug-in for UNIXです。



SnapCenterでホストイニシエータとの近接性をサポートするには、この値（sourceまたはdestination）をONTAPで設定する必要があります。

SnapCenterでサポートされていないユースケース:

- ONTAPでSnapMirrorアクティブ同期関係のポリシーを *automatedfailover* から *automatedfailoverduplex* に変更して、既存の非対称SnapMirrorアクティブ同期ワークロードを対称に変換しても、SnapCenterでは同じことはサポートされません。
- リソース グループのバックアップ (SnapCenterですでに保護されている) があり、ONTAPでSnapMirrorアクティブ同期関係のストレージ ポリシーが *automatedfailover* から *automatedfailoverduplex* に変更された場合、同じことはSnapCenterではサポートされません。

データ保護の主要概念

SnapCenterを使用する前に、バックアップ、クローン、復元の主要な概念を理解してください。

リソース

リソースには、データベース、Windows ファイル システム、またはSnapCenterでバックアップまたはクローンされたファイル共有が含まれます。環境によっては、リソースはデータベース インスタンス、SQL Server 可用性グループ、Oracle データベース、RAC データベース、またはカスタム アプリケーション グループになることもあります。

リソース グループ

リソース グループは、ホストまたはクラスター上のリソースのコレクションであり、複数のホストおよびクラスターからのリソースが含まれる場合があります。リソース グループに対して実行された操作は、指定されたスケジュールに基づいてそのすべてのリソースに適用されます。個々のリソースまたはグループに対して、オンデマンドまたはスケジュールされたバックアップを実行できます。



共有リソース グループ内の 1 つのホストがメンテナンス モードに入ると、そのグループのすべてのスケジュールされた操作がすべてのホストで中断されます。

特定のリソースをバックアップするには、データベースの場合はデータベース プラグイン、ファイル システムの場合はファイル システム プラグイン、VM およびデータストアの場合はSnapCenter Plug-in for VMware vSphereなどの関連プラグインを使用します。

ポリシー

ポリシーは、バックアップの頻度、コピーの保持、レプリケーション、スクリプト、およびデータ保護操作のその他の特性を指定します。

リソース グループを作成するとき、またはオンデマンド バックアップを実行するときに、1 つ以上のポリシーを選択できます。

リソース グループは、保護する必要がある内容と、日時に基づいていつ保護する必要があるかを定義します。ポリシーでは、保護がどのように実行されるかを説明します。たとえば、ホストのすべてのデータベースまたはファイル システムをバックアップする必要がある場合、ホスト内のすべてのデータベースまたはファイル システムを含むリソース グループが作成されることがあります。その後、日次ポリシーと時間別ポリシ

一の 2 つのポリシーをリソース グループに適用できます。

リソース グループを作成してポリシーをアタッチするときに、毎日完全バックアップを実行し、1 時間ごとにログ バックアップを実行する別のスケジュールを構成することができます。

データ保護操作では、カスタムのプレスクリプトとポストスクリプトを使用できます。これらのスクリプトを使用すると、データ保護ジョブの前または後に自動化を行うことができます。たとえば、スクリプトはデータ保護ジョブの失敗や警告を自動的に通知できます。プレスクリプトとポストスクリプトを設定する前に、これらのスクリプトを作成するための要件を理解することが重要です。

序文と後書きの使い方

カスタムのプレスクリプトとポストスクリプトを使用すると、ジョブの前または後にデータ保護タスクを自動化できます。たとえば、ジョブの失敗や警告を通知するスクリプトを追加できます。設定する前に、これらのスクリプトの要件を理解していることを確認してください。

サポートされるスクリプト タイプ

Windowsでは、次の種類のスクリプトがサポートされています。

- バッチ ファイル
- PowerShellのスクリプト
- Perlスクリプト

UNIXでは、次の種類のスクリプトがサポートされています。

- Perlスクリプト
- Pythonスクリプト
- シェル スクリプト



デフォルトのBashシェルに加えて、shシェル、kシェル、cシェルなど他のシェルもサポートされています。

スクリプト パス

非仮想化ストレージ システムと仮想化ストレージ システムの両方でSnapCenter操作の一部として実行されるすべての事前スクリプトと事後スクリプトは、プラグイン ホストで実行されます。

- Windowsスクリプトが、プラグイン ホスト上にある必要があります。



プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

- UNIXスクリプトが、プラグイン ホスト上にある必要があります。



スクリプト パスは、実行時に検証されます。

スクリプトを指定する場所

スクリプトはバックアップ ポリシーに指定します。バックアップ ジョブが開始されると、ポリシーによってスクリプトがバックアップ対象のリソースに自動的に関連付けられます。バックアップ ポリシーの作成時に、プリスクリプトとポストスクリプトの引数を指定できます。



複数のスクリプトを指定することはできません。

スクリプトのタイムアウト

デフォルトでは、タイムアウトは60秒に設定されています。タイムアウト値は変更できます。

スクリプト出力

Windowsでは、プリスクリプトとポストスクリプトの出力ファイルが格納されるデフォルト ディレクトリは、Windows\System32です。

UNIXには、プリスクリプトとポストスクリプトが格納されるデフォルトの場所はありません。出力ファイルは、任意の場所にリダイレクトできます。

SnapCenterでサポートされるストレージ システムとアプリケーション

SnapCenterでサポートされているストレージ システム、アプリケーション、およびデータベースを知っておく必要があります。

サポートされているストレージシステム

- NetApp ONTAP 9.12.1以降
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

Non-Volatile Memory Express (NVMe) over Transport Control Protocol (TCP) をサポートします。

Amazon FSx for NetApp ONTAPの詳細については、以下を参照してください。 ["Amazon FSx for NetApp ONTAPドキュメント"](#)。

- NetApp ONTAP 9.16.1 を実行しているNetApp ASA r2 システム。

サポートされているアプリケーションとデータベース

SnapCenterでは、さまざまなアプリケーションやデータベースの保護がサポートされています。サポートされているアプリケーションとデータベースの詳細については、以下を参照してください。 ["NetApp Interoperability Matrix Tool"](#)。

SnapCenter は、VMware Cloud on Amazon Web Services (AWS) ソフトウェア定義データセンター (SDDC) 環境での Oracle および Microsoft SQL ワークロードの保護をサポートします。 <https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-Oracle-MS-SQL-workloads-using-NetApp-SnapCenter-in-VMware-Cloud-on-AWS/ba-p/449168> [詳細情報[^]]。

SnapCenter資格情報の認証方法

資格情報では、アプリケーションや環境に応じて異なる認証方法が使用されます。資格情報により、ユーザーは認証され、SnapCenter の操作を実行できるようになります。プラグインのインストール用とデータ保護操作用の資格情報セットをそれぞれ 1 セット作成する必要があります。

Windows認証

Windows認証方式は、Active Directoryに照らして認証します。Windows 認証の場合、Active Directory はSnapCenterの外部に設定されます。SnapCenter は追加の構成なしで認証します。ホストを追加したり、プラグイン パッケージをインストールしたり、ジョブをスケジュールしたりするには、Windows 資格情報が必要です。

信頼されないドメインの認証

SnapCenterでは、信頼されていないドメインに属するユーザーとグループが Windows 資格情報を作成できます。認証を成功させるには、信頼されていないドメインをSnapCenterに登録する必要があります。

ローカル ワークグループ認証

SnapCenter を使用すると、ローカル ワークグループのユーザーとグループを使用して Windows 資格情報を作成できます。ローカル ワークグループ ユーザーおよびグループの Windows 認証は、Windows 資格情報の作成中には実行されず、ホストの登録やその他のホスト操作が実行されるまで延期されます。

SQL Server認証

SQL認証方式は、SQL Serverインスタンスに照らして認証します。したがって、SQL ServerインスタンスがSnapCenterで検出されなければなりません。そのため、SQLクレデンシャルを追加する前に、ホストの追加とプラグイン パッケージのインストールを完了し、リソースをリフレッシュしておく必要があります。SQL Server でのスケジュール設定やリソースの検出などの操作を実行するには、SQL Server 認証が必要です。

Linux認証

Linux認証方式は、Linuxホストに照らして認証します。Linux認証は、SnapCenter GUIからリモートでLinuxホストを追加してSnapCenter Plug-ins Package for Linuxをインストールする際の最初のステップで必要になります。

AIX認証

AIX認証方式は、AIXホストに照らして認証します。AIX認証は、SnapCenter GUIからリモートでAIXホストを追加してSnapCenter Plug-ins Package for AIXをインストールする際の最初のステップで必要になります。

Oracleデータベース認証

Oracleデータベース認証方式は、Oracleデータベースに照らして認証します。Oracleデータベース認証は、Oracleデータベースに対する処理を実行する際、データベース ホストでオペレーティング システム（OS）認証が無効になっている場合に必要になります。したがって、Oracle データベース資格情報を追加する前に、Oracle データベースに sysdba 権限を持つ Oracle ユーザーを作成する必要があります。

Oracle ASM認証

Oracle ASM認証方式は、Oracle Automatic Storage Management (ASM) インスタンスに照らして認証します。Oracle ASM インスタンスにアクセスする必要があり、データベース ホストで OS 認証が無効になっている場合は、Oracle ASM 認証が必要です。Oracle ASM 資格情報を追加する前に、ASM インスタンスにシステム権限を持つ Oracle ユーザーを作成します。

RMANカタログ認証

RMANカタログ認証方式は、Oracle Recovery Manager (RMAN) カタログ データベースに照らして認証します。外部のカタログ メカニズムを設定し、データベースをカタログ データベースに登録している場合は、RMANカタログ認証を追加する必要があります。

ASA r2 システムでサポートされているSnapCenter操作

ASA r2 ストレージ システムは、SnapCenter 6.1 以降でサポートされます。 ["ASA r2 システムの詳細"](#)

SnapCenter は、ZAPI をサポートしていないASA r2 システム上のすべての操作を REST API を利用して実行します。

- ASA r2 システム用のSnapCenterでサポートされている操作*
- VMDK 経由でアプリケーションのプライマリ バックアップを作成する
- 整合性グループのスナップショットをセカンダリストレージシステムに転送する
- プライマリおよびセカンダリストレージシステムから元のホストまたは代替ホストへのバックアップの復元
 - VMware vMotionを使用したプライマリおよびセカンダリストレージシステムからのインプレースリストア
 - プライマリおよびセカンダリストレージシステムの両方から接続してコピーを復元します
- バックアップを元のホストまたは代替ホストに複製する

SnapCenter は、ONTAP整合性グループを検出または作成できます。また、二次保護のために宛先クラスタへのSnapMirror関係をプロビジョニングおよび初期化することもできます。

アプリケーションに対してASA r2 システムで二次保護を有効にする方法については、以下を参照してください。

- ["Microsoft SQL Server リソースの二次保護を有効にする"](#)
- ["SAP HANAリソースの二次保護を有効にする"](#)
- ["Oracleリソースの二次保護を有効にする"](#)
- ["Windows ファイルシステムの二次保護を有効にする"](#)
- ["IBM Db2 リソースの二次保護を有効にする"](#)
- ["PostgreSQLリソースの二次保護を有効にする"](#)
- ["MySQLリソースの二次保護を有効にする"](#)
- ["Unix ファイルシステムの二次保護を有効にする"](#)

- ASA r2 システムではSnapCenterではサポートされていない操作*
- RAWデバイスマッピング (RDM)
- Oracleのアプリケーションボリューム
- SAP HANA NDV
- ロックボルト
- 改ざん防止スナップショット
- FlexGroupボリューム
- 階層的整合性グループ
- ASA、AFF、またはFASストレージ システムからASA r2ストレージ システムへの移行
- ASA、AFF、またはFASリソースとASA r2リソースが混在するデータベースの保護
- スナップショットの名前変更
- SQLプラグインホストのログディレクトリの二次プロビジョニング

SnapCenter softwareのクイック スタート

クイック スタート ガイドでは、SnapCenter softwareをインストールして構成するための基本的な手順について説明します。

1

SnapCenter Serverのインストールの準備

SnapCenter Server をインストールするためのすべての要件が満たされていることを確認する必要があります。

- ["要件"](#)
- ["SnapCenter softwareにアクセスするには登録してください"](#)
- ["多要素認証の有効化"](#)

2

SnapCenterサーバーをインストールする

SnapCenter Server は、Windows ホストまたは Linux ホストにインストールできます。 SnapCenter Serverのインストールパッケージを以下のサイトからダウンロードします。 ["NetAppサポート サイト"](#)インストーラーを実行します。

- ["WindowsにSnapCenterサーバーをインストールする"](#)
- ["LinuxにSnapCenter Serverをインストールする"](#)

3

SnapCenterサーバーを構成する

SnapCenter Server をインストールした後、環境に応じて構成する必要があります。

4

アプリケーション用のプラグインをインストールする

使用しているアプリケーションに基づいて、アプリケーション固有のプラグインをインストールするためのすべての要件が満たされていることを確認してから、それぞれのプラグインのインストールを続行します。

5

アプリケーションを保護する

SnapCenter Server と必要なプラグインを正常にインストールしたら、アプリケーション バックアップの作成を開始できます。これらのバックアップは、後で必要に応じて復元やクローン作成の目的で利用できます。

SnapCenter Serverのインストールと構成

SnapCenter Serverのインストールの準備

SnapCenter Server をインストールするための要件

Windows または Linux ホストにSnapCenter Server をインストールする前に、環境のすべての要件が満たされていることを確認する必要があります。

Windowsホストのドメインとワークグループの要件

SnapCenter Server は、ドメインまたはワークグループ内の Windows ホストにインストールできます。

管理者権限を持つユーザーは、SnapCenterサーバーをインストールできます。

- Active Directory ドメイン: ローカル管理者権限を持つドメイン ユーザーを使用する必要があります。ドメイン ユーザーは、Windowsホストのローカル管理者グループのメンバーである必要があります。
- ワークグループ: ローカル管理者権限を持つローカル アカウントを使用する必要があります。

ドメイン トラスト、マルチドメイン フォレスト、およびクロスドメイン トラストはサポートされていますが、クロスフォレスト ドメインはサポートされません。詳細については、Active Directoryドメインと信頼に関するMicrosoftのドキュメントを参照してください。



SnapCenter Server をインストールした後は、SnapCenterホストが配置されているドメインを変更しないでください。SnapCenter Server がインストールされたときに存在していたドメインからSnapCenter Server ホストを削除し、その後SnapCenter Server をアンインストールしようとすると、アンインストール操作は失敗します。

スペースとサイジングの要件

スペースとサイズの要件をよく理解しておく必要があります。

項目	Windowsホストの要件	Linuxホストの要件
オペレーティング システム	Microsoft Windows サポートされているのは、英語版、ドイツ語版、日本語版、簡体字中国語版のみです。 サポートされているバージョンに関する最新情報については、 https://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT[\"NetApp Interoperability Matrix Tool\"] 。	• Red Hat Enterprise Linux (RHEL) 8および9 • SUSE Linux Enterprise Server (SLES) 15 サポートされているバージョンに関する最新情報については、 https://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT[\"NetApp Interoperability Matrix Tool\"] 。
最小CPU数	4	4

項目	Windowsホストの要件	Linuxホストの要件
最小RAM	8 GB  MySQL Serverのバッファ プールがRAMの20%を使用します。	8 GB
最小ハード ドライブ スペース - SnapCenter Serverソフトウェアおよびログ用	7 GB  SnapCenter Server がインストールされているドライブと同じドライブにSnapCenterリポジトリがある場合は、15 GBを使用することを推奨します。	15 GB
最小ハード ドライブ スペース - SnapCenterリポジトリ用	8 GB  注意: SnapCenterリポジトリがインストールされているドライブと同じドライブにSnapCenter Server がある場合は、15 GB を用意することをお勧めします。	該当なし
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell 7.4.2以降	• .NET Framework 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) • PowerShell 7.4.2以降 • Nginxはリバース プロキシとして使用できるWebサーバ • Pam-devel PAM (Pluggable Authentication Modules) は、システム管理者が、認証を行うプログラムを再コンパイルすることなく認証ポリシーを設定できるようにするシステム セキュリティ ツールです。



ASP.NET コアでは、Windows 上の SnapCenter Server の一時ファイル システムにアクセスするために IIS_IUSRS が必要です。

SANホストの要件

SnapCenter にはホスト ユーティリティや DSM は含まれていません。SnapCenterホストが SAN (FC/iSCSI) 環境の一部である場合は、SnapCenter Server ホストに追加のソフトウェアをインストールして構成する必要があります。

- ホスト ユーティリティ: ホスト ユーティリティは FC と iSCSI をサポートしており、Windows サーバーで MPIO を使用できるようになります。 ["詳細情報"](#)。
- Microsoft DSM for Windows MPIO: このソフトウェアは Windows MPIO ドライバーと連携して、NetApp と Windows ホスト コンピューター間の複数のパスを管理します。ハイアベイラビリティ構成にはDSMが必要です。



ONTAP DSMを使用していた場合は、Microsoft DSMに移行する必要があります。詳細については、以下を参照してください。 ["ONTAP DSMからMicrosoft DSMへの移行方法"](#)。

ブラウザの要件

SnapCenter softwareは、Chrome 125 以降および Microsoft Edge 110.0.1587.17 以降をサポートしています。

ポート要件

SnapCenter softwareでは、異なるコンポーネント間の通信に異なるポートが必要です。

- 1つのポートを複数のアプリケーションで共有することはできません。
- デフォルト ポートを使用しない場合は、インストール時にカスタム ポートを選択できます。
- 固定ポートの場合は、デフォルトのポート番号を受け入れる必要があります。
- ファイアウォール
 - ファイアウォール、プロキシ、またはその他のネットワーク デバイスによって接続が妨げられないように注意してください。
 - SnapCenter をインストールするときにカスタム ポートを指定する場合は、SnapCenterプラグインローダーのそのポートのファイアウォール ルールをLoaderイン ホストに追加する必要があります。

次の表に、各ポートとそのデフォルト値をまとめています。

ポート名	ポート番号	プロトコル	送受信方向	説明
SnapCenterのポート	8146	HTTPS	双方向	このポートは、SnapCenterクライアント (SnapCenter ユーザー) と SnapCenter Server 間の通信に使用され、プラグインホストから SnapCenter Server への通信にも使用されます。 ポート番号をカスタマイズできます。
SnapCenter SMCoreの通信ポート	8145	HTTPS	双方向	このポートは、SnapCenter Server と SnapCenter プラグインがインストールされているホスト間の通信に使用されます。 ポート番号をカスタマイズできます。
スケジューラ サービス ポート	8154	HTTPS		このポートは、SnapCenter Serverホスト内で管理されるすべてのプラグインのSnapCenterスケジューラのワークフローを一元的にオーケストレーションするために使用されます。 ポート番号をカスタマイズできます。
RabbitMQ ポート	5672	TCP		これは RabbitMQ がリッスンするデフォルトのポートであり、Scheduler サービスと SnapCenter 間のパブリッシャー - サブスクライバーモデル通信に使用されます。

ポート名	ポート番号	プロトコル	送受信方向	説明
MySQLのポート	3306	HTTPS		このポートは、SnapCenterリポジトリ データベースとの通信に使用されます。 SnapCenter サーバーから MySQL サーバーへの安全な接続を作成できます。 "詳細情報"
Windows プラグイン ホスト	135, 445	TCP		このポートは、SnapCenter Server とプラグインがインストールされているホスト間の通信に使用されます。 Microsoft によって指定された追加の動的ポート範囲も開いている必要があります。
Linux / AIX プラグイン ホスト	22	SSH	一方向	このポートは、サーバからクライアントホストに開始される、 SnapCenter サーバとホスト間の通信に使用されます。
Windows、Linux、AIX 用の SnapCenter プラグイン パッケージ	8145	HTTPS	双方向	このポートは、SMCore とプラグイン パッケージがインストールされているホスト間の通信に使用されます。 カスタマイズ可能。 ポート番号をカスタマイズできます。
SnapCenter Plug-in for Oracle Database	27216			デフォルトのJDBCポートは、Oracleデータベースに接続するためにOracle用プラグインで使用されます。

ポート名	ポート番号	プロトコル	送受信方向	説明
SnapCenter Plug-in for Exchange Database	909			デフォルトのNET.TCPポートは、Exchange VSS コールバックに接続するためにPlug-in for Windowsで使用されます。
NetAppでサポートされるSnapCenter用プラグイン	9090	HTTPS		これはプラグインホストでのみ使用される内部ポートであり、ファイアウォールの例外は必要ありません。 SnapCenterサーバーとプラグイン間の通信は、ポート 8145 を介してルーティングされます。
ONTAPクラスタまたはSVMの通信ポート	• 443 (HTTPS) • 80 (HTTP)	• HTTPS • HTTP	双方向	このポートは、SnapCenter Serverを実行するホストとSVMの間の通信のためにSAL (Storage Abstraction Layer) で使用されます。また、現在は、SnapCenterプラグインホストとSVMの間の通信のためにSnapCenter for WindowsプラグインホストのSALでも使用されます。
SnapCenter Plug-in for SAP HANA Database	• 3インスタンス番号13 • 3インスタンス番号15	• HTTPS • HTTP	双方向	マルチテナント データベース コンテナ (MDC) のシングル テナントの場合、ポート番号は13で終わります。MDC以外の場合、ポート番号は15で終わります。 ポート番号をカスタマイズできます。

ポート名	ポート番号	プロトコル	送受信方向	説明
SnapCenter Plug-in for PostgreSQL	5432			このポートは、PostgreSQL 用プラグインが PostgreSQL クラスターと通信するために使用されるデフォルトの PostgreSQL ポートです。 ポート番号をカスタマイズできます。

SnapCenterソフトウェアにアクセスするための登録

Amazon FSx for NetApp ONTAPまたはAzure NetApp Filesを初めて使用し、既存のNetAppアカウントを持っていない場合は、SnapCenter softwareにアクセスするために登録する必要があります。

開始する前に

- 会社のEメールIDにアクセスできる必要があります。
- Azure NetApp Filesを使用している場合は、AzureサブスクリプションIDが必要です。
- Amazon FSx for NetApp ONTAPを使用している場合は、FSx for ONTAPファイルシステムのファイルシステムIDが必要です。

タスク概要

登録には情報検証が必要であり、確認と新しいNetAppサポート サイト (NSS) アカウントの ゲスト アクセス から フル アクセスへのアップグレードには最大 1 日かかる場合があります。

手順

1. クリック <https://mysupport.netapp.com/site/user/registration>登録用。
2. 会社のメール ID を入力し、キャプチャを完了し、NetApp のプライバシー ポリシーに同意して、[送信] をクリックします。
3. メール ID に送信された OTP を入力して登録を認証し、「続行」をクリックします。
4. 登録完了ページで、以下の情報を入力して登録を完了します。
 - a. * NetApp顧客/エンドユーザー* を選択します。
 - b. [シリアル番号] フィールドに、Azure NetApp Files を使用している場合は Azure サブスクリプション ID を入力し、Amazon FSx for NetApp ONTAPを使用している場合はファイル システム ID を入力します。



チケットを申請するには <https://mysupport.netapp.com/site/help>登録中に問題が発生した場合、またはステータスを知りたい場合。

多要素認証 (MFA)

多要素認証 (MFA) の管理

Active Directory フェデレーション サービス (AD FS) サーバと SnapCenter Server で多要素認証 (MFA) 機能を管理できます。

多要素認証 (MFA) の有効化

SnapCenter Server の MFA 機能は、PowerShell コマンドを使用して有効にできます。

タスク概要

- 同じ AD FS に他のアプリケーションが設定されている場合、SnapCenter は SSO ベースのログインをサポートします。セキュリティ上の理由から、一部の AD FS 構成では、AD FS セッションの永続化に応じて、SnapCenter でユーザ認証が必要になる場合があります。
- コマンドレットで使用できるパラメータとその説明に関する情報は、以下を実行することで取得できます。Get-Help command_name。あるいは、"[SnapCenter ソフトウェア コマンドレット リファレンス ガイド](#)"。

開始する前に

- Windows Active Directory フェデレーション サービス (AD FS) が、それぞれのドメインで稼働している必要があります。
- Azure MFA や Cisco Duo など、AD FS でサポートされている多要素認証サービスが必要です。
- SnapCenter Server と AD FS サーバのタイムスタンプは、タイムゾーンに関係なく同じにする必要があります。
- SnapCenter Server 用に、承認済みの CA 証明書を取得して設定します。

CA 証明書は、次の理由で必須です。

- 自己署名証明書はノード レベルで一意であるため、ADFS と F5 間の通信が切断されないようにします。
- スタンドアロン構成または高可用性構成でのアップグレード、修復、ディザスタ リカバリ (DR) の実行中に自己署名証明書が再作成されないようにして、MFA の再設定を回避します。
- IP-FQDN の解決を保証します。

CA 証明書の詳細については、"[CA 証明書 CSR ファイルの生成](#)"。

手順

1. Active Directory フェデレーション サービス (AD FS) のホストに接続します。
2. AD FS フェデレーションメタデータファイルを以下からダウンロードします。"<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>" です。
3. ダウンロードしたファイルを SnapCenter Server にコピーして、MFA 機能を有効にします。
4. PowerShell を使用して、SnapCenter 管理者ユーザとして SnapCenter Server にログインします。
5. PowerShell セッションで、`New-SmMultifactorAuthenticationMetadata -path` コマンドレットを使用して SnapCenter MFA メタデータ ファイルを生成します。

pathパラメータには、SnapCenter ServerのホストにMFAメタデータ ファイルを保存するためのパスを指定します。

6. 生成されたファイルをAD FSのホストにコピーし、SnapCenterをクライアント エンティティとして設定します。
7. SnapCenter ServerのMFAを有効にするには、`Set-SmMultiFactorAuthentication` コマンドレット。
8. (オプション) MFAの構成ステータスと設定を確認するには、`Get-SmMultiFactorAuthentication` コマンドレット。
9. Microsoft管理コンソール (MMC) に移動し、次の手順を実行します。
 - a. ファイル > *スナップインの追加と削除* をクリックします。
 - b. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
 - c. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
 - d. コンソール ルート > 証明書 - ローカル コンピューター > 個人 > 証明書 をクリックします。
 - e. SnapCenterにバインドされた CA 証明書を右クリックし、[すべてのタスク] > [秘密キーの管理] を選択します。
 - f. アクセス許可ウィザードで、次の手順を実行します。
 - i. *[追加]* をクリックします。
 - ii. *場所* をクリックし、該当するホスト (階層の最上位) を選択します。
 - iii. *場所* ポップアップウィンドウで *OK* をクリックします。
 - iv. オブジェクト名フィールドに「IIS_IUSRS」と入力し、[名前の確認] をクリックして、[OK] をクリックします。

チェックが成功した場合は、[OK] をクリックします。

10. AD FSホストでAD FS管理ウィザードを開き、次の手順を実行します。
 - a. 証明書利用者信頼 > 証明書利用者信頼の追加 > 開始 を右クリック。
 - b. 2 番目のオプションを選択し、SnapCenter MFA メタデータ ファイルを参照して、[次へ] をクリックします。
 - c. 表示名を指定して、[次へ] をクリックします。
 - d. 必要に応じてアクセス制御ポリシーを選択し、「次へ」をクリックします。
 - e. 次のタブの設定をデフォルトに設定します。
 - f. *[完了]* をクリックします。

SnapCenterが、指定した表示名の証明書利用者として反映されます。

11. 名前を選択し、次の手順を実行します。
 - a. *クレーム発行ポリシーの編集* をクリックします。
 - b. *ルール of 追加* をクリックし、*次へ* をクリックします。
 - c. 要求規則の名前を指定します。

- d. 属性ストアとして*Active Directory*を選択します。
- e. 属性として*User-Principal-Name*を選択し、出力クレームの種類として*Name-ID*を選択します。
- f. *[完了]*をクリックします。

12. ADFSサーバで、次のPowerShellコマンドを実行します。

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'  
-SigningCertificateRevocationCheck None
```

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'  
-EncryptionCertificateRevocationCheck None
```

13. 次の手順を実行して、メタデータがインポートされたことを確認します。

- a. 証明書利用者信頼を右クリックし、[プロパティ]を選択します。
- b. [エンドポイント]、[識別子]、[署名]フィールドに値が入力されていることを確認します。

14. すべてのブラウザ タブを閉じ、ブラウザを再度開いて既存の、またはアクティブなセッションCookieをクリアし、再度ログインします。

SnapCenterのMFA機能は、REST APIを使用して有効にすることもできます。

トラブルシューティング情報については、["複数のタブで同時にログインしようとすると、MFAエラーが表示されます"](#)。

AD FS MFAメタデータの更新

アップグレード、CA証明書の更新、DRなど、AD FSサーバに何らかの変更があった場合は、SnapCenterでAD FS MFAメタデータを更新する必要があります。

手順

1. AD FSフェデレーションメタデータファイルを以下からダウンロードします。"<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>"
2. ダウンロードしたファイルをSnapCenter Serverにコピーして、MFAの設定を更新します。
3. 次のコマンドレットを実行して、SnapCenterでAD FSメタデータを更新します。

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. すべてのブラウザ タブを閉じ、ブラウザを再度開いて既存の、またはアクティブなセッションCookieをクリアし、再度ログインします。

SnapCenter MFAメタデータの更新

修復、CA証明書の更新、DRなど、ADFSサーバに何らかの変更があった場合は、AD FSでSnapCenter MFAメタデータを更新する必要があります。

手順

1. AD FSホストでAD FS管理ウィザードを開き、次の手順を実行します。
 - a. *証明書利用者信頼*を選択します。
 - b. SnapCenter用に作成された証明書利用者信頼を右クリックし、[削除]を選択します。

証明書利用者信頼のユーザ定義名が表示されます。

- c. 多要素認証 (MFA) を有効にします。

見る["多要素認証を有効にする"](#)。

2. すべてのブラウザ タブを閉じ、ブラウザを再度開いて既存の、またはアクティブなセッションCookieをクリアし、再度ログインします。

多要素認証 (MFA) の無効化

手順

1. MFAを無効にし、MFAが有効になったときに作成された構成ファイルをクリーンアップします。`Set-SmMultiFactorAuthentication` コマンドレット。
2. すべてのブラウザ タブを閉じ、ブラウザを再度開いて既存の、またはアクティブなセッションCookieをクリアし、再度ログインします。

REST API、PowerShell、SCCLIを使用した多要素認証 (MFA) の管理

MFAログインは、ブラウザ、REST API、PowerShell、およびSCCLIでサポートされます。MFAはAD FS ID マネージャーを通じてサポートされます。GUI、REST API、PowerShell、SCCLIを使用して、MFAの有効化、MFAの無効化、およびMFAの設定を行うことができます。

AD FSのOAuth / OIDCとしてのセットアップ

Windows GUIウィザードを使用してAD FSを構成する

1. サーバー マネージャー ダッシュボード > ツール > **ADFS** 管理 に移動します。
2. **ADFS** > アプリケーション グループ に移動します。
 - a. アプリケーション グループ を右クリックします。
 - b. アプリケーション グループの追加 を選択し、アプリケーション名 を入力します。
 - c. *サーバーアプリケーション*を選択します。
 - d. *次へ*をクリックします。
3. *クライアント識別子*をコピーします。

これがクライアントIDです。..[リダイレクトURI]にコールバックURL (SnapCenter ServerのURL) を追加します。..*次へ*をクリックします。

4. *共有シークレットの生成*を選択します。

シークレット値をコピーします。これがクライアントのシークレットです。..*次へ*をクリックします。

5. *概要*ページで*次へ*をクリックします。
 - a. *完了*ページで*閉じる*をクリックします。
6. 新しく追加された*アプリケーション グループ*を右クリックし、*プロパティ*を選択します。

7. アプリのプロパティから*アプリケーションの追加*を選択します。

8. *アプリケーションを追加*をクリックします。

Web APIを選択し、[次へ]をクリックします。

9. [Web APIの構成]ページで、SnapCenter ServerのURLと前の手順で作成したクライアントIDを[識別子]セクションに入力します。

a. *[追加]*をクリックします。

b. *次へ*をクリックします。

10. *アクセス制御ポリシーの選択*ページで、要件に基づいて制御ポリシーを選択し (たとえば、すべてのユーザーを許可し、MFAを要求する)、*次へ*をクリックします。

11. *アプリケーションの権限の構成*ページでは、デフォルトで openid がスコープとして選択されているので、*次へ*をクリックします。

12. *概要*ページで*次へ*をクリックします。

*完了*ページで*閉じる*をクリックします。

13. サンプル アプリケーションのプロパティ ページで、**OK** をクリックします。

14. 承認サーバ (AD FS) によって発行され、リソースによって消費されることを意図したJWTトークン。

このトークンの「aud」つまりオーディエンス要求は、リソースまたはWeb APIの識別子と一致している必要があります。

15. 選択したWebAPIを編集し、コールバックURL (SnapCenter ServerのURL) とクライアント識別子が正しく追加されていることを確認します。

ユーザ名を要求として提供するようにOpenID Connectを設定します。

16. サーバー マネージャーの右上にある ツール メニューの下にある **AD FS 管理** ツールを開きます。

a. 左側のサイドバーから*アプリケーション グループ* フォルダを選択します。

b. Web API を選択し、[編集] をクリックします。

c. [発行変換規則]タブに移動します。

17. *ルールの追加*をクリックします。

a. クレーム ルール テンプレートのドロップダウンで、**LDAP** 属性をクレームとして送信 を選択します。

b. *次へ*をクリックします。

18. *クレームルール*の名前を入力します。

a. 属性ストアのドロップダウンで*Active Directory*を選択します。

b. **LDAP** 属性 ドロップダウンで **User-Principal-Name** を選択し、送信クレーム タイプ ドロップダウンで **UPN** を選択します。

c. *[完了]*をクリックします。

PowerShellコマンドを使用したアプリケーション グループの作成

PowerShellコマンドを使用して、アプリケーション グループ、Web APIを作成し、スコープと要求を追加できます。これらのコマンドは、自動スクリプト形式で使用できます。詳細については、<KB 記事へのリンク>を参照してください。

1. 次のコマンドを使用して、AD FSに新しいアプリケーション グループを作成します。

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier  
-ApplicationGroupIdentifier $ClientRoleIdentifier
```

`ClientRoleIdentifier`アプリケーショングループの名前

`redirectURL`承認後のリダイレクト用の有効なURL

2. AD FSサーバ アプリケーションを作成し、クライアント シークレットを生成します。

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"  
-ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL  
-Identifier $identifier -GenerateClientSecret
```

3. ADFS Web APIアプリケーションを作成し、使用するポリシー名を設定します。

```
$identifier = (New-Guid).Guid
```

```
Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier  
-Name "App Web API"
```

```
-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. クライアントIDとクライアント シークレットは1回しか表示されないため、次のコマンドの出力から取得します。

```
"client_id = $identifier"
```

```
"client_secret: "$($ADFSApp.ClientSecret)
```

5. AD FSアプリケーションにallatclaims権限とopenid権限を付与します。

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier  
-ServerRoleIdentifier $identifier -ScopeNames @('openid')
```

```
$transformrule = @"
```

```
@RuleTemplate = "LdapClaims"
```

```
@RuleName = "AD User properties and Groups"
```

```
c:[Type ==  
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",  
Issuer ==
```

```
"AD AUTHORITY"]
```

```
⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. 変換規則ファイルを書き出します。

```
$transformrule | Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii
$relativePath = Get-Item .\issueancetransformrules.tmp
```

7. Web APIアプリケーションに名前を付け、外部ファイルを使用してその発行変換規則を定義します。

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

アクセス トークンの有効期限の更新

PowerShellコマンドを使用して、アクセス トークンの有効期限を更新できます。

このタスクについて

- アクセス トークンは、ユーザ、クライアント、およびリソースの特定の組み合わせに対してのみ使用できます。アクセス トークンは無効にすることはできず、期限切れになるまで有効です。
- デフォルトでは、アクセス トークンの有効期間は60分です。最小値の有効期間でも十分な長さになるよう設定されています。現在進行中のビジネス クリティカルなジョブが妨げられないように、十分な値を指定する必要があります。

ステップ

アプリケーション グループWebAPIのアクセス トークンの有効期限を更新するには、AD FSサーバで次のコマンドを使用します。

```
+
Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"
```

AD FSからのBearerトークンの取得

RESTクライアント（Postmanなど）で以下のパラメータを入力する必要があります。RESTクライアントからユーザ クレデンシャルを入力するように求められます。さらに、ベアラー トークンを取得するには、2 要素認証（ユーザが所有している情報と、ユーザが何者であるか）を入力する必要があります。

+ ベアラー トークンの有効期間はアプリケーションごとに AD FS サーバーから構成可能で、デフォルトの有効期間は 60 分です。

フィールド	Value

助成金の種類	Authorization Code
Callback URL	コールバックURLがない場合は、アプリケーションのベースURLを入力します。
Auth URL	[adfsドメイン名]/adfs/oauth2/authorize
Access token URL	[adfsドメイン名]/adfs/oauth2/トークン
クライアントID	AD FSクライアントIDを入力します。
Client secret	AD FSクライアント シークレットを入力します。
Scope	OpenID
クライアント認証	Send as Basic AUTH Header
リソース	詳細オプション タブで、コールバック URL と同じ値を持つリソース フィールドを追加します。この値は、JWT トークンの "aud" 値として提供されます。

PowerShell、SCCLI、REST APIを使用したSnapCenter ServerでのMFAの設定

PowerShell、SCCLI、およびREST APIを使用して、SnapCenter ServerでMFAを設定できます。

SnapCenter MFA CLI認証

PowerShellとSCCLIでは、既存のコマンドレット（Open-SmConnection）を「AccessToken」という追加のフィールドで拡張し、Bearerトークンを使用してユーザを認証します。

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port <String>] [-RoleName <String>] [-AccessToken <string>]
```

上記のコマンドレットを実行すると、それぞれのユーザがSnapCenterコマンドレットを実行できるようにセッションが作成されます。

SnapCenter MFA REST API認証

REST API クライアント (Postman や swagger など) で *Authorization=Bearer <access token>* の形式のベアラー トークンを使用し、ヘッダーにユーザーの RoleName を指定して、 SnapCenterから正常な応答を取得します。

MFA REST APIのワークフロー

MFAがAD FSで設定されている場合、REST APIを使用してSnapCenterアプリケーションにアクセスするには、アクセス (Bearer) トークンを使用して認証する必要があります。

このタスクについて

- Postman、Swagger UI、FireCampなど、任意のRESTクライアントを使用できます。
- アクセス トークンを取得し、それを使用して以降の要求（SnapCenter REST API）を認証し、任意の処理を実行します。

手順

AD FS MFA 経由で認証するには

1. AD FSエンドポイントを呼び出してアクセス トークンを取得するようにRESTクライアントを設定します。

ボタンを押してアプリケーションのアクセス トークンを取得すると、AD FS SSOページにリダイレクトされます。そのページでADクレデンシャルを入力してMFAで認証する必要があります。1.AD FS SSOページで、[Username]テキスト ボックスにユーザ名または電子メールを入力します。

+ ユーザー名は、user@domain または domain\user の形式にする必要があります。

2. [Password]テキスト ボックスにパスワードを入力します。
3. *ログイン*をクリックします。
4. サインイン オプション セクションから認証オプションを選択し、認証します (構成によって異なります)。
 - プッシュ: 携帯電話に送信されるプッシュ通知を承認します。
 - QRコード: AUTH Pointモバイルアプリを使用してQRコードをスキャンし、アプリに表示される確認コードを入力します。
 - ワンタイム パスワード: トークンのワンタイム パスワードを入力します。

5. 認証が成功すると、アクセス、ID、およびリフレッシュ トークンを含むポップアップが表示されます。

アクセス トークンをコピーし、SnapCenter REST APIで使用して操作を実行します。

6. REST APIのヘッダー セクションでアクセス トークンとロール名を渡す必要があります。
7. AD FSから取得したこのアクセス トークンをSnapCenterが検証します。

有効なトークンである場合、SnapCenterはそのトークンをデコードし、ユーザ名を取得します。

8. SnapCenterがユーザ名とロール名を使用して、API実行のためにユーザ認証を行います。

認証に成功した場合、SnapCenterは結果を返します。失敗した場合は、エラー メッセージが表示されます。

REST API、CLI、GUIのSnapCenter MFA機能の有効化または無効化

GUI

手順

1. SnapCenter管理者としてSnapCenter Serverにログインします。

2. 設定 > グローバル設定 > *多要素認証(MFA)設定*をクリックします
3. インターフェイス（GUI / REST API / CLI）を選択してMFAログインを有効または無効にします。

PowerShell インターフェース

手順

1. GUI、REST API、PowerShell、SCCLIのMFAを有効にするためのPowerShellコマンドまたはCLIコマンドを実行します。

```
Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled  
-IsCliMFAEnabled -Path
```

pathパラメータには、AD FS MFAメタデータxmlファイルの場所を指定します。

SnapCenter GUI、REST API、PowerShell、およびSCCLIが、指定したAD FSメタデータ ファイル パスを使用して設定され、MFAが有効になります。

2. MFAの構成ステータスと設定を確認するには、`Get-SmMultiFactorAuthentication` コマンドレット。

SCCLI インターフェース

手順

1. # sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true
-IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path
"C:\ADFS_metadata\abc.xml"
2. # sccli Get-SmMultiFactorAuthentication

REST API

1. GUI、REST API、PowerShell、SCCLIのMFAを有効にするには、次のPOST APIを実行します。

パラメータ	Value
要求のURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	投稿
要求の本文	{ "IsGuiMFAEnabled": false、 "IsRestApiMFAEnabled": true、 "IsCliMFAEnabled": false、 "ADFSConfigFilePath": "C:\ADFS_metadata\abc.xml" }

応答の本文	{ "MFAConfiguration": { "IsGuiMFAEnabled": false、 "ADFSSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null、 "IsRestApiMFAEnabled": true、 "IsCliMFAEnabled": false、 "ADFSSHostName": "win-adsf- sc49.winscedom2.com" } }

2. 次のAPIを使用して、MFAのステータスと設定を確認します。

パラメータ	Value
要求のURL	/api/4.9/settings/multifactorauthentication
HTTPメソッド	Get
応答の本文	{ "MFAConfiguration": { "IsGuiMFAEnabled": false、 "ADFSSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null、 "IsRestApiMFAEnabled": true、 "IsCliMFAEnabled": false、 "ADFSSHostName": "win-adsf- sc49.winscedom2.com" } }

SnapCenter Serverのインストール

WindowsホストへのSnapCenter Serverのインストール

SnapCenter Serverインストーラの実行ファイルを使用して、SnapCenter Serverをインストールできます。

必要に応じて、PowerShellコマンドレットを使用して複数のインストール手順や設定手順を実行することもできます。PowerShell 7.4.2 以降を使用する必要があります。



コマンドラインからのSnapCenter Serverのサイレント インストールは、サポートされていません。

開始する前に

- SnapCenter ServerホストにWindowsの最新の更新プログラムが適用されていて、システムの再起動が完了している必要があります。
- SnapCenter ServerをインストールするホストにMySQL Serverがインストールされていないことを確認しておく必要があります。
- Windowsインストーラのデバッグを有効にしておく必要があります。

有効化の詳細については、MicrosoftのWebサイトを参照してください。 ["Windowsインストーラのログ"](#)。



Microsoft Exchange Server、Active Directory、またはドメイン ネーム サーバが配置されたホストには、SnapCenter Serverをインストールしないでください。

手順

1. SnapCenter Serverのインストールパッケージを以下からダウンロードします。 "[NetAppサポート サイト](#)"。
2. ダウンロードした.exeファイルをダブルクリックして、SnapCenter Serverのインストールを開始します。

インストールを開始すると、すべての事前確認が実行されます。最小要件を満たしていない場合は、対応するエラーまたは警告メッセージが表示されます。

警告メッセージは無視してインストールを続行できますが、エラーは修正する必要があります。

3. SnapCenter Serverのインストールに必要な入力済みの値を確認し、必要に応じて変更します。

MySQL Serverリポジトリ データベースのパスワードを指定する必要はありません。SnapCenter Serverのインストール時には、パスワードが自動生成されます。



特殊文字「%`」 is not supported in the custom path for the repository database. If you include "`パスに「%」が含まれていると、インストールは失敗します。

4. *今すぐインストール*をクリックします。

無効な値を指定すると、対応するエラー メッセージが表示されます。値を再入力してからインストールを開始してください。



*キャンセル*ボタンをクリックすると、実行中のステップが完了し、ロールバック操作が開始されます。SnapCenter Serverはホストから完全に削除されます。

ただし、「SnapCenter Server サイトの再起動」または「SnapCenter Server の起動を待機中」の操作の実行中に [キャンセル] をクリックすると、操作はキャンセルされずにインストールが続行されます。

ログ ファイルは常にadminユーザの%temp%フォルダに（古い順に）表示されます。ログの場所をリダイレクトする場合は、次のコマンドを実行して、コマンド プロンプトからSnapCenter Server のインストールを開始します。C:\installer_location\installer_name.exe /log"C:\\"

インストール中に **Windows** ホストで有効になる機能

SnapCenter Serverインストーラでのインストール中、WindowsホストでWindowsの機能とロールが有効になります。これらは、ホスト システムのトラブルシューティングと保守に役立つ可能性があります。

カテゴリ	特徴
Webサーバー	• インターネット インフォメーション サービス • World Wide Webサービス • HTTP共通機能 ◦ 既定のドキュメント ◦ ディレクトリの参照 ◦ HTTPエラー ◦ HTTPリダイレクション ◦ 静的なコンテンツ ◦ WebDAV発行 • 状態と診断 ◦ カスタム ログ ◦ HTTPログ ◦ ログ ツール ◦ 要求監視 ◦ トレース • パフォーマンス機能 ◦ 静的なコンテンツの圧縮 • セキュリティ ◦ IPセキュリティ ◦ 基本認証 ◦ 一元的なSSL証明書のサポート ◦ クライアント証明書マッピング認証 ◦ IIS クライアント証明書マッピング認証 ◦ IPおよびドメインの制限 ◦ 要求フィルター ◦ URL承認 ◦ Windows認証 • アプリケーション開発機能 ◦ .NET拡張機能4.5 ◦ アプリケーションの初期化 ◦ ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティングバンドル ◦ サーバー側インクルード WebSocketプロトコル
	管理ツール

カテゴリ	特徴
IIS管理スクリプトおよびツール	• IIS管理サービス • Web管理ツール
.NET Framework 8.0.12 の機能	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • Windows Communication Foundation (WCF) HTTP Activation⁴⁵ ◦ TCPアクティブ化 ◦ HTTPアクティブ化
メッセージ キュー	• メッセージ キュー サービス  SnapCenterで作成および管理するMSMQサービスが他のアプリケーションで使用されていないことを確認してください。 • RabbitMQ • Erlang
Windowsプロセス アクティブ化サービス	• プロセス モデル
構成API	All

LinuxホストへのSnapCenter Serverのインストール

SnapCenter Serverインストーラの実行ファイルを使用して、SnapCenter Serverをインストールできます。

開始する前に

- SnapCenterをインストールするための十分な権限がないroot以外のユーザを使用してSnapCenter Serverをインストールする場合は、NetAppサポート サイトからsudoersチェックサム ファイルを入手します。Linuxのバージョンに基づいて適切なチェックサム ファイルを使用する必要があります。
- SUSE Linuxでsudoパッケージを使用できない場合は、認証の失敗を回避するためにsudoパッケージをインストールします。
- SUSE Linuxの場合は、インストールの失敗を回避するためにホスト名を設定します。
- 次のコマンドを実行して、Linuxのセキュアステータスを確認します。 `sestatus`。 **SELinux** ステータスが「有効」で、現在のモード が「強制」の場合は、次の操作を実行します。
 - 次のコマンドを実行します。 `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

_WEBAPP_EXTERNAL_PORT_のデフォルト値は8146です。

- ファイアウォールがポートをブロックしている場合は、`sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

_WEBAPP_EXTERNAL_PORT_のデフォルト値は8146です。

- 読み取りおよび書き込み権限があるディレクトリから、次のコマンドを実行します。

- `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

コマンドから「nothing to do」が返された場合は、SnapCenter Serverのインストール後にコマンドを再実行します。

- コマンドによって *my-nginx.pp* が作成された場合は、次のコマンドを実行してポリシー パッケージをアクティブにします。 `sudo semodule -i my-nginx.pp`

- MySQL PID ディレクトリに使用されるパスは */var/opt/mysqld* です。次のコマンドを実行して、MySQLインストールの権限を設定します。

- `mkdir /var/opt/mysqld`

- `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`

- `sudo restorecon -Rv /var/opt/mysqld`

- MySQL データ ディレクトリに使用されるパスは、*/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/* です。次のコマンドを実行して、MySQL データ ディレクトリの権限を設定します。

- `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

- `sudo semanage fcontext -a -t mysqld_db_t
"/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`

- `sudo restorecon -Rv
/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

タスク概要

- SnapCenter ServerをLinuxホストにインストールすると、MySQL、RabbitMQ、Erllangなどのサードパーティ サービスがインストールされます。これらはアンインストールしないでください。
- LinuxホストにインストールされているSnapCenter Serverは、以下をサポートしていません。
 - 高可用性
 - Windowsプラグイン
 - Active Directory（ローカル ユーザ[クレデンシャルを持つrootユーザおよびroot以外のユーザ]のみをサポート）
 - SnapCenterへのログインに使用するキーベースの認証
- .NET ランタイムのインストール中に、*libicu* ライブラリの依存関係を解決できない場合は、次のコマンドを実行して *libicu* をインストールします。 `yum install -y libicu`
- *Perl* が利用できないためにSnapCenter Server のインストールが失敗する場合は、次のコマンドを実行して *Perl* をインストールします。 `yum install -y perl`

手順

1. 以下からダウンロードしてください "[NetAppサポート サイト](#)"/home ディレクトリ へ。
 - SnapCenter Server インストール パッケージ - **snapcenter-linux-server-(el8/el9/sles15).bin**
 - 公開鍵ファイル - **snapcenter_public_key.pub**
 - それぞれの署名ファイル - **snapcenter-linux-server-(el8/el9/sles15).bin.sig**
2. 署名ファイルを検証します。

```
$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>
```
3. 非ルート ユーザーによるインストールの場合は、.bin インストーラーに付属する **snapcenter_server_checksum_(el8/el9/sles15).txt** に指定されている visudo コンテンツを追加します。
4. .bin インストーラーの実行権限を割り当てます。

```
chmod +x snapcenter-linux-server-(el8/el9/sles15).bin
```
5. いずれかの操作を実行して、SnapCenter Serverをインストールします。

実行する処理	操作
対話型インストール	<pre>./snapcenter-linux-server-(el8/el9/sles15).bin</pre> 次の情報を入力するように求められます。 • Linuxホスト外部のSnapCenter Serverにアクセスするために使用されるWebApp外部ポート。デフォルト値は8146です。 • SnapCenter ServerをインストールするSnapCenter Serverユーザ。 • パッケージがインストールされるインストールディレクトリ。

実行する処理	操作
非対話型インストール	<pre> sudo ./snapcenter-linux-server- (e18/e19/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename> </pre> 例: <code>sudo ./snapcenter_linux_server.bin -i silent</code> <code>-DWEBAPP_EXTERNAL_PORT=8146</code> <code>-DSNAPCENTER_SERVER_USER=root</code> <code>-DUSER_INSTALL_DIR=/opt</code> <code>-DINSTALL_LOG_NAME=InstallerLog.log</code> ログは <code>/var/opt/snapcenter/logs</code> に保存されます。 SnapCenter Serverをインストールするために渡されるパラメータ： • <code>DWEBAPP_EXTERNAL_PORT</code>: Linux ホスト外部のSnapCenter Server にアクセスするために使用される Web アプリケーション外部ポート。デフォルト値は8146です。 • <code>DWEBAPP_INTERNAL_PORT</code>: Linux ホスト内のSnapCenter Server にアクセスするために使用される Web アプリケーションの内部ポート。デフォルト値は8147です。 • <code>DSMCORE_PORT</code>: smcore サービスが実行されている SMCORE ポート。デフォルト値は8145です。 • <code>DSCHEDULER_PORT</code>: スケジューラ サービスが実行されているスケジューラ ポート。デフォルト値は8154です。 • <code>DSNAPCENTER_SERVER_USER</code>: SnapCenter Server をインストールするSnapCenter Server ユーザー。 <code>DSNAPCENTER_SERVER_USER</code> の場合、デフォルトはインストーラーを実行しているユーザーです。 • <code>DUSER_INSTALL_DIR</code>: パッケージがインストールされるインストール ディレクトリ。 <code>DUSER_INSTALL_DIR</code> の場合、デフォルトのインストール ディレクトリは <code>/opt</code> です。 • <code>DINSTALL_LOG_NAME</code>: インストール ログが保存されるログ ファイル名。これはオプションパラメータで、指定した場合はコンソールにログが表示されなくなります。このパラメータを指定しない場合は、ログがコンソールに表示され、デフォルトのログ ファイルにも保存されます。

次の手順

- SELinux ステータスが「有効」で、現在のモードが「強制」の場合、nginx サービスは起動に失敗します。次のコマンドを実行する必要があります。
 - a. ホーム ディレクトリに移動します。
 - b. 次のコマンドを実行します。 `journalctl -x | grep -i nginx` に割り当てる必要があります。デフォルト値は0です。
 - c. WebApp内部ポート（8147）でリッスンできない場合は、次のコマンドを実行します。
 - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
 - `semodule -i my-nginx.pp`
 - d. 走る `setsebool -P httpd_can_network_connect on`

インストール中にLinuxホストで有効になる機能

SnapCenter Server は、ホスト システムのトラブルシューティングとメンテナンスに役立つ以下のソフトウェア パッケージをインストールします。

- Rabbitmq
- Erlang

SnapCenterを登録する

NetApp製品を初めて使用し、既存のNetAppアカウントを持っていない場合は、サポートを有効にするためにSnapCenterを登録する必要があります。

手順

1. SnapCenterをインストールした後、*ヘルプ> バージョン情報*に移動します。
2. [SnapCenter について] ダイアログ ボックスで、971 で始まる 20 桁の番号であるSnapCenterインスタンスをメモします。
3. クリック <https://register.netapp.com>。
4. 私は**NetApp**の登録顧客ではありません をクリックします。
5. ご自身の情報を指定して、登録します。
6. [NetApp Reference SN]フィールドは空白のままにします。
7. 製品ラインドロップダウンから* SnapCenter*を選択します。
8. 課金プロバイダを選択します。
9. 20桁のSnapCenterインスタンスIDを入力します。
10. *送信*をクリックします。

RBAC許可を使用したSnapCenterへのログイン

SnapCenterでは、ロールベース アクセス制御（RBAC）がサポートされています。SnapCenter管理者は、SnapCenter RBACを使用して、ロールとリソースをワークグループ / Active Directory内のユーザまたはActive Directory内のグループに割り当てま

す。RBACユーザは、割り当てられたロールを使用してSnapCenterにログインできるようになりました。

開始する前に

- Windowsサーバ マネージャでWindowsプロセス アクティビ化サービス（WAS）を有効にする必要があります。
- Internet Explorerをブラウザとして使用してSnapCenter Serverにログインする場合は、Internet Explorerの保護モードが無効になっていることを確認する必要があります。
- SnapCenter ServerがLinuxホストにインストールされている場合は、SnapCenter Serverのインストールに使用したユーザ アカウントを使用してログインする必要があります。

このタスクについて

インストール時には、SnapCenter Serverのインストール ウィザードによってショートカットが作成され、SnapCenterがインストールされているホストのデスクトップと[スタート]メニューに配置されます。また、インストールが終了すると、インストール ウィザードに、インストール時に指定した情報に基づいてSnapCenterのURLが表示されます。リモート システムからログインする場合は、このURLをコピーして使用できます。



Webブラウザで複数のタブを開いている場合は、SnapCenterのブラウザ タブだけを閉じて、SnapCenterからはログアウトされません。SnapCenterとの接続を終了するには、[サインアウト] ボタンをクリックするか、Web ブラウザ全体を閉じて、SnapCenterからログアウトする必要があります。

ベスト プラクティス: セキュリティ上の理由から、ブラウザでSnapCenter のパスワードを保存しないようにすることをお勧めします。

デフォルトの GUI URL は、SnapCenter Server がインストールされているサーバーのデフォルト ポート 8146 への安全な接続です (<https://server:8146>)。SnapCenterのインストール時に別のサーバ ポートを指定した場合は、そのポートが代わりに使用されます。

高可用性 (HA) 展開の場合、仮想クラスター IP https://Virtual_Cluster_IP_or_FQDN:8146 を使用してSnapCenterにアクセスする必要があります。Internet Explorer (IE) で https://Virtual_Cluster_IP_or_FQDN:8146 に移動してもSnapCenter UI が表示されない場合は、各プラグインホストの IE で仮想クラスターの IP アドレスまたは FQDN を信頼済みサイトとして追加するか、各プラグインホストで IE セキュリティ強化を無効にする必要があります。詳細については、以下を参照してください。 "[ネットワーク外からクラスタIPアドレスにアクセスできない](#)"。

SnapCenter GUIに加えて、PowerShellコマンドレットを使用してスクリプトを作成し、設定、バックアップ、リストアの各処理を実行できます。一部のコマンドレットは、SnapCenterの各リリースで変更されている場合があります。その "[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"詳細が記載されています。



SnapCenterへの初回ログイン時は、インストール プロセスで指定したクレデンシャルを使用してログインする必要があります。

手順

1. ローカル ホストのデスクトップに表示されたショートカット、インストールの終了時に表示されたURL、またはSnapCenter管理者から受け取ったURLを使用して、SnapCenterを起動します。

2. ユーザ クレデンシャルを入力します。

指定する項目	使用する形式
ドメイン管理者	• NetBIOS\UserName • UserName@UPN suffix 例：username@netapp.com • Domain FQDN\UserName
ローカル管理者	UserName

3. 複数のロールが割り当てられている場合は、このログイン セッションで使用するロールを[ロール]ボックスから選択します。

ログインすると、SnapCenterの右上に現在のユーザとそのロールが表示されます。

結果

[Dashboard]ページが表示されます。

サイトにアクセスできないというエラーでログ記録が失敗した場合は、SSL 証明書をSnapCenterにマップする必要があります。 ["詳細情報"](#)

終わったら

SnapCenter Serverに初めてRBACユーザとしてログインしたら、リソース リストを更新します。

SnapCenterでサポート対象にする信頼されないActive Directoryドメインがある場合は、信頼されないドメインのユーザにロールを設定する前に、それらのドメインをSnapCenterに登録する必要があります。 ["詳細情報"](#)。

Linux ホスト上で実行されているSnapCenterにプラグイン ホストを追加する場合は、`/opt/NetApp/snapcenter/SnapManagerWeb/Repository` の場所からチェックサム ファイルを取得する必要があります。

6.0リリース以降では、デスクトップにSnapCenter PowerShellのショートカットが作成されます。ショートカットを使用すると、SnapCenter PowerShellコマンドレットに直接アクセスできます。

多要素認証（MFA）を使用した**SnapCenter**へのログイン

SnapCenter Serverは、Active Directoryに含まれているドメイン アカウントのMFAをサポートしています。

開始する前に

MFAを有効にしておく必要があります。MFAを有効にする方法については、以下を参照してください。 ["多要素認証を有効にする"](#)

このタスクについて

- FQDNのみがサポートされます。

- ワークグループ ユーザとクロスドメイン ユーザは、MFAを使用したログインはできません。

手順

1. ローカル ホストのデスクトップに表示されたショートカット、インストールの終了時に表示されたURL、またはSnapCenter管理者から受け取ったURLを使用して、SnapCenterを起動します。
2. AD FSのログイン ページで、ユーザ名とパスワードを入力します。

AD FSのページに、ユーザ名またはパスワードが無効だというエラー メッセージが表示された場合は、次の点を確認してください。

- 有効なユーザ名とパスワードであるかどうか

ユーザ アカウントがActive Directory (AD) に存在している必要があります。

- ADで設定された最大試行回数を超えていないかどうか
- ADとAD FSが稼働中かどうか

SnapCenterのデフォルトのGUIセッション タイムアウトの変更

SnapCenter GUIのセッション タイムアウト時間を、デフォルトのタイムアウト時間である20分から変更できます。

セキュリティ機能として、デフォルトでは、操作を行わないまま15分が経過すると、5分後にSnapCenterのGUIセッションからログアウトすることを示す警告が表示されます。また、操作を行わないまま20分が経過すると、SnapCenterのGUIセッションからログアウトされ、再度ログインが必要になります。

手順

1. 左側のナビゲーション ペインで、[設定] > [グローバル設定] をクリックします。
2. [グローバル設定]ページで、[構成設定]をクリックします。
3. [セッション タイムアウト] フィールドに新しいセッション タイムアウトを分単位で入力し、[保存] をクリックします。

SSL 3.0の無効化によるSnapCenter Webサーバの保護

SnapCenter WebサーバでSecure Socket Layer (SSL) 3.0プロトコルが有効になっている場合は、セキュリティ上の理由からMicrosoft IISで無効にする必要があります。

SSL 3.0プロトコルには欠陥があり、攻撃者が悪用して接続エラーを引き起こしたり、中間者攻撃を実行したり、Webサイトと訪問者の間の暗号化トラフィックを監視したりすることができます。

手順

1. SnapCenter Web サーバー ホストでレジストリ エディターを起動するには、[スタート] > [実行] をクリックし、「regedit」と入力します。
2. レジストリ エディタ
で、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\に移動します。

- サーバー キーがすでに存在する場合:
 - i. 有効な DWORD を選択し、[編集] > [変更] をクリックします。
 - ii. 値を 0 に変更し、[OK] をクリックします。
- サーバーキーが存在しない場合は:
 - i. 編集 > 新規 > キー をクリックし、キーに Server という名前を付けます。
 - ii. 新しいサーバー キーを選択した状態で、[編集] > [新規] > [DWORD] をクリックします。
 - iii. 新しいDWORDに「Enabled」という名前を付け、値として「0」を入力します。

3. レジストリ エディタを閉じます。

SnapCenterサーバーを構成する

ストレージシステムの追加とプロビジョニング

ストレージシステムを追加する

データ保護およびプロビジョニング操作を実行するには、SnapCenter がONTAPストレージ、ASA r2 システム、またはAmazon FSx for NetApp ONTAPにアクセスできるようにストレージ システムをセットアップする必要があります。

スタンドアロンのSVMを追加するか、複数のSVMで構成されるクラスタを追加できます。Amazon FSx for NetApp ONTAPを使用している場合は、fsxadminアカウントを使用して複数のSVMで構成されるFSx管理LIFを追加したり、SnapCenterでFSx SVMを追加したりできます。

開始する前に

- ストレージ接続を作成するには、Infrastructure Adminロールの権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

ストレージ システム接続の追加中は、ホスト プラグインのインストールが進行中であってはなりません。ホスト キャッシュが更新されず、SnapCenter GUI にデータベースのステータスが「バックアップに使用できません」または「NetAppストレージ上にありません」と表示される可能性があるためです。

- ストレージ システムの名前は一意である必要があります。

SnapCenterでは、別々のクラスタに属している場合でも、複数のストレージ システムに同じ名前を付けることはサポートされません。SnapCenterでサポートする各ストレージ システムには、一意な名前とデータLIFの一意なIPアドレスが必要です。

このタスクについて

- ストレージ システムの設定時に、イベント管理システム（EMS）とAutoSupportの機能を有効にすることもできます。AutoSupportツールは、システムの健全性に関するデータを収集し、そのデータをシステムのトラブルシューティング用にNetAppテクニカル サポートに自動的に送信します。

これらの機能を有効にすると、リソースが保護されたとき、リストアやクローンの処理が完了したとき、または処理が失敗したときに、SnapCenterからストレージ システムにAutoSupport情報が、ストレージ システムのsyslogにEMSメッセージが送信されます。

- SnapMirrorデスティネーションまたはSnapVaultデスティネーションにSnapshotをレプリケートする場合は、デスティネーションSVM / クラスタとソースSVM / クラスタへのストレージ システム接続をセットアップする必要があります。



ストレージ システムのパスワードを変更すると、スケジュール済みジョブ、オンデマンド バックアップ、およびリストア処理が失敗する場合があります。ストレージ システムのパスワードを変更した後、[ストレージ] タブで [変更] をクリックしてパスワードを更新できます。

手順

1. 左側のナビゲーション ペインで、[ストレージ システム] をクリックします。
2. ストレージ システム ページで、[新規] をクリックします。
3. [Add Storage System] ページで、次の情報を入力します。

フィールド	操作
Storage System	ストレージ システムの名前またはIPアドレスを入力します。 ストレージ システム名（ドメイン名は含めない）は15文字以下にする必要があります。解決可能な名前を使用してください。15文字を超える名前のストレージ システム接続を作成する場合は、Add-SmStorageConnectionPowerShell コマンドレットを使用します。 MetroCluster 構成（MCC）のストレージ システムでノンストップ オペレーションを実現するには、ローカル クラスタとピア クラスタの両方を登録することを推奨します。 SnapCenterでは、別々のクラスタに属している場合でも、複数のSVMに同じ名前を付けることはサポートされません。SnapCenterでサポートするSVMには、すべて一意の名前を付ける必要があります。 SnapCenterにストレージ接続を追加したあとで、ONTAPを使用してSVMまたはクラスタの名前を変更しないでください。 SVMに短縮名またはFQDNを追加した場合は、その名前がSnapCenterとプラグイン ホストの両方から解決できる必要があります。

フィールド	操作
ユーザー名/パスワード	ストレージ システムへのアクセスに必要な権限を持つストレージ ユーザのクレデンシャルを入力します。
Event Management System (EMS) & AutoSupport Settings	保護が適用されたとき、リストア処理が完了したとき、または処理が失敗したときにEMSメッセージをストレージ システムのsyslogに送信、またはAutoSupportメッセージをストレージ システムに送信するには、該当するチェックボックスをオンにします。 失敗した操作に関するAutoSupport通知をストレージ システムに送信する チェックボックスをオンにすると、AutoSupport通知を有効にするには EMS メッセージングが必要であるため、* SnapCenter Server イベントを syslog に記録する* チェックボックスもオンになります。

4. プラットフォーム、プロトコル、ポート、タイムアウトに割り当てられたデフォルト値を変更する場合は、[その他のオプション] をクリックします。

- a. [Platform]で、ドロップダウン リストから次のいずれかのオプションを選択します。

SVM がバックアップ関係におけるセカンダリ ストレージ システムである場合は、[セカンダリ] チェックボックスをオンにします。セカンダリ オプションを選択すると、SnapCenter はライセンス チェックをすぐに実行しません。

SnapCenterでSVMを追加した場合は、ドロップダウンからプラットフォーム タイプを手動で選択する必要があります。

- a. [Protocol]で、SVMまたはクラスタのセットアップ時に設定したプロトコル（通常はHTTPS）を選択します。
 - b. ストレージ システムが受け入れるポートを入力します。

通常はデフォルト ポート443を使用します。

- c. 接続を試行する時間（秒）を入力します。

デフォルト値は60秒です。

- d. SVM に複数の管理インターフェイスがある場合は、[優先 IP] チェックボックスをオンにし、SVM 接続の優先 IP アドレスを入力します。

- e. *保存*をクリックします。

5. *送信*をクリックします。

結果

[ストレージ システム] ページの [タイプ] ドロップダウンから、次のいずれかのアクションを実行します。

- 追加されたすべての SVM を表示する場合は、* ONTAP SVM* を選択します。

FSx SVMを追加した場合は、ここにFSx SVMが表示されます。

- 追加されたすべてのクラスタを表示する場合は、* ONTAPクラスタ* を選択します。

fsxadminを使用してFSxクラスタを追加した場合は、ここにFSxクラスタが表示されます。

クラスタ名をクリックすると、そのクラスタに含まれるすべてのSVMが[Storage Virtual Machine]セクションに表示されます。

ONTAP GUI を使用してONTAPクラスタに新しい SVM が追加された場合は、[再検出] をクリックして新しく追加された SVM を表示します。

終わったら

SnapCenterがアクセスできるすべてのストレージ システムからEメール通知を送信するには、クラスタ管理者が各ストレージ システム ノードでAutoSupportを有効にする必要があります。ストレージ システムのコマンドラインで次のコマンドを実行してください。

```
autosupport trigger modify -node nodename -autosupport-message client.app.info
-to enable -noteto enable
```



Storage Virtual Machine (SVM) 管理者にはAutoSupportへのアクセス権はありません。

ストレージ接続とクレデンシャル

データ保護処理を実行する前に、ストレージ接続をセットアップし、SnapCenter Server とSnapCenterプラグインで使用するクレデンシャルを追加する必要があります。

ストレージ接続

SnapCenter ServerとSnapCenterプラグインは、ストレージ接続を通じてONTAPストレージにアクセスします。SVM接続を設定するには、AutoSupport機能およびイベント管理システム (EMS) 機能も設定する必要があります。

Credentials

- ドメイン管理者または管理者グループの任意のメンバー

ドメイン管理者またはSnapCenterプラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。ユーザ名フィールドの有効な形式は次のとおりです。

- NetBIOS\ユーザー名
- ドメインFQDN\ユーザー名
- ユーザー名@upn

- ローカル管理者 (ワークグループの場合のみ)

ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト シス

テムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザ アカウントを指定できます。

ユーザー名フィールドの有効な形式は次のとおりです: *UserName*

- 個々のリソース グループのクレデンシャル

個々のリソース グループのクレデンシャルを設定する場合で、ユーザ名に完全なadmin権限が割り当てられていない場合は、少なくともリソース グループとバックアップの権限を割り当てる必要があります。

Windowsホストでのストレージのプロビジョニング

igroupの作成と管理

イニシエータ グループ (igroup) を作成して、ストレージ システム上の特定のLUNにアクセスできるホストを指定することができます。SnapCenterを使用して、Windows ホスト上の igroup を作成、名前変更、変更、または削除できます。

igroupの作成

SnapCenterを使用して、Windows ホスト上に igroup を作成できます。igroup を LUN にマップすると、ディスクの作成ウィザードまたはディスクの接続ウィザードで igroup が使用できるようになります。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、**igroup** をクリックします。
3. イニシエーター グループ ページで、[新規] をクリックします。
4. [igroup の作成] ダイアログ ボックスで、igroup を定義します。

フィールド	操作
Storage System	igroup にマップする LUN の SVM を選択します。
ホスト	igroupを作成するホストを選択します。
グループ名	igroupの名前を入力します。
イニシエーター	イニシエータを選択します。
タイプ	イニシエータ タイプとして、iSCSI、FCP、または混在（FCPとiSCSI）のいずれかを選択します。

5. 入力内容に満足したら、「**OK**」をクリックします。

SnapCenter はストレージ システム上に igroup を作成します。

igroupの名前の変更

SnapCenterを使用して、既存の igroup の名前を変更できます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、**igroup** をクリックします。
3. [イニシエータ グループ] ページで、[ストレージ仮想マシン] フィールドをクリックして使用可能な SVM のリストを表示し、名前を変更する igroup の SVM を選択します。
4. SVM の igroup のリストで、名前を変更する igroup を選択し、「名前の変更」をクリックします。
5. 「igroup の名前変更」ダイアログ ボックスで、igroup の新しい名前を入力し、「名前の変更」をクリックします。

igroupの変更

SnapCenter を使用して、既存の igroup に igroup イニシエーターを追加できます。igroupの作成時に追加できるホストは1つだけです。クラスタに対してigroupを作成するには、既存のigroupを変更して他のノードを追加します。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、**igroup** をクリックします。
3. [イニシエータ グループ] ページで、[ストレージ仮想マシン] フィールドをクリックして使用可能な SVM のドロップダウン リストを表示し、変更する igroup の SVM を選択します。
4. igroup のリストで igroup を選択し、「**igroup** にイニシエーターを追加」をクリックします。
5. ホストを選択します。
6. イニシエーターを選択し、[OK] をクリックします。

igroupを削除する

不要になった igroup は、SnapCenterを使用して削除できます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、**igroup** をクリックします。
3. [イニシエータ グループ] ページで、[ストレージ仮想マシン] フィールドをクリックして使用可能な SVM のドロップダウン リストを表示し、削除する igroup の SVM を選択します。
4. SVM の igroup のリストで、削除する igroup を選択し、[削除] をクリックします。
5. 「igroup の削除」ダイアログボックスで、「**OK**」をクリックします。

SnapCenter はigroup を削除します。

Windowsホストは、ストレージ システム上のLUNを仮想ディスクとして認識します。SnapCenterを使用して、FC接続LUNまたはiSCSI接続LUNを作成および設定できます。

- SnapCenterでサポートされるのは、ベーシック ディスクのみです。ダイナミック ディスクはサポートされていません。
- GPTでは1つのデータ パーティションのみ、MBRではNTFSまたはCSVFSでフォーマットされた1つのボリュームと1つのマウント パスを持つ1つのプライマリ パーティションのみを含めることができます。
- サポートされているパーティション スタイル: GPT、MBR。VMware UEFI VM では、iSCSI ディスクのみがサポートされます。



SnapCenterでは、ディスクの名前を変更することはできません。SnapCenterで管理しているディスクの名前が変更された場合、SnapCenterの処理は正常に実行されません。

ホスト上のディスクの表示

SnapCenterで管理している各Windowsホスト上のディスクを表示できます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. *ホスト*ド롭ダウンリストからホストを選択します。

ディスクのリストが表示されます。

クラスタ ディスクの表示

SnapCenterで管理しているクラスタ上のクラスタ ディスクを表示できます。クラスタ ディスクは、[Hosts] ドロップダウンからクラスタを選択した場合にのみ表示されます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. ホスト ドロップダウン リストからクラスターを選択します。

ディスクのリストが表示されます。

iSCSIセッションの確立

iSCSIを使用してLUNに接続する場合は、LUNを作成して通信を有効にする前に、iSCSIセッションを確立する必要があります。

始める前に

- ストレージ システムのノードをiSCSIターゲットとして定義しておく必要があります。
- ストレージ システムで iSCSI サービスを開始する必要があります。 ["詳細情報"](#)

このタスクについて

iSCSIセッションは、同じバージョンのIP間（IPv6とIPv6またはIPv4とIPv4）でのみ確立できます。

リンクローカルIPv6アドレスは、iSCSIセッションの管理や、ホストとターゲットの間の通信（ホストとターゲットが両方とも同じサブネット内に存在する場合）に使用できます。

iSCSIイニシエータの名前を変更すると、iSCSIターゲットへのアクセスに影響します。名前を変更した場合、新しい名前が認識されるように、イニシエータがアクセスするターゲットの再設定が必要になることがあります。iSCSIイニシエータの名前を変更した場合、ホストを必ず再起動してください。

ホストに複数の iSCSI インターフェイスがある場合、最初のインターフェイスの IP アドレスを使用してSnapCenterへの iSCSI セッションを確立すると、別の IP アドレスを持つ別のインターフェイスから iSCSI セッションを確立することはできません。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[iSCSI セッション] をクリックします。
3. ストレージ仮想マシン ドロップダウン リストから、iSCSI ターゲットのストレージ仮想マシン (SVM) を選択します。
4. *ホスト*ドロップダウンリストから、セッションのホストを選択します。
5. *セッションの確立*をクリックします。

セッションの確立ウィザードが表示されます。

6. セッションの確立ウィザードで、ターゲットを特定します。

フィールド	入力する内容
ターゲットノード名	iSCSIターゲットのノード名 既存のターゲット ノードがある場合、表示されるノード名は変更できません。
ターゲットポータルアドレス	ターゲット ネットワーク ポータルのIPアドレス
ターゲットポータルポート	ターゲット ネットワーク ポータルのTCPポート
イニシエーターポータルアドレス	イニシエータ ネットワーク ポータルのIPアドレス

7. 入力内容に満足したら、「接続」をクリックします。

SnapCenter はiSCSI セッションを確立します。

8. 同じ手順を繰り返して各ターゲットのセッションを確立します。

FC接続またはiSCSI接続のLUNまたはディスクの作成

Windowsホストは、ストレージ システム上のLUNを仮想ディスクとして認識します。SnapCenterを使用して、FC接続LUNまたはiSCSI接続LUNを作成および設定できます。

SnapCenterの外部でディスクを作成してフォーマットする場合は、NTFSファイルシステムとCSVFSファイルシステムのみがサポートされます。

開始する前に

- ストレージ システム上にLUN用のボリュームを作成しておく必要があります。

このボリュームには、SnapCenterで作成したLUNのみを格納します。



SnapCenterで作成したクローン ボリュームには、クローンがすでにスプリットされている場合を除き、LUNを作成することはできません。

- ストレージ システムでFCサービスまたはiSCSIサービスを開始しておく必要があります。
- iSCSIを使用している場合は、ストレージ システムとのiSCSIセッションを確立しておく必要があります。
- SnapCenter Plug-ins Package for Windowsをインストールする必要があるのは、ディスクを作成するホストだけです。

このタスクについて

- Windows Serverフェイルオーバー クラスタ内のホストで共有する場合を除き、LUNを複数のホストに接続することはできません。
- Cluster Shared Volume (CSV; クラスタ共有ボリューム) を使用したWindows Serverフェイルオーバー クラスタ内のホストでLUNを共有する場合、クラスタ グループを所有するホストにディスクを作成する必要があります。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. *ホスト*ドロップダウンリストからホストを選択します。
4. *新規*をクリックします。

[Create Disk]ウィザードが開きます。

5. [LUN Name]ページで、LUNの情報を指定します。

フィールド	操作
Storage System	LUNのSVMを選択します。

フィールド	操作
LUN path	参照 をクリックして、LUN を含むフォルダーの完全なパスを選択します。
LUN名	LUNの名前を入力します。
Cluster size	クラスタのLUNのブロック割り当てサイズを選択します。 クラスタのサイズは、オペレーティング システムおよびアプリケーションによって異なります。
LUN label	必要に応じて、LUNの説明を入力します。

6. [Disk Type]ページで、ディスク タイプを選択します。

選択するオプション	状況
Dedicated disk	LUNにアクセスできるホストは1つだけです。 リソース グループ フィールドは無視します。
共有ディスク	Windows Serverフェイルオーバー クラスタ内のホストでLUNを共有します。 リソース グループ フィールドにクラスター リソース グループの名前を入力します。ディスクはフェイルオーバー クラスタ内の1つのホストだけに作成します。
Cluster Shared Volume (CSV)	CSVを使用するWindows Serverフェイルオーバー クラスタ内のホストでLUNを共有します。 リソース グループ フィールドにクラスター リソース グループの名前を入力します。ディスクはクラスター グループを所有するホストに作成する必要があります。

7. [Drive Properties]ページで、ドライブのプロパティを指定します。

プロパティ	説明
マウントポイントの自動割り当て	システム ドライブに基づいて、SnapCenterで自動的にボリューム マウント ポイントを割り当てます。 たとえば、システム ドライブがC:であれば、C:ドライブにボリューム マウント ポイント (C:\scmntpt\l) が作成されます。自動割り当ては共有ディスクではサポートされません。
Assign drive letter	ドロップダウン リストで選択したドライブにディスクをマウントします。
Use volume mount point	フィールドで指定したドライブ パスにディスクをマウントします。 ボリューム マウント ポイントのルートは、ディスクを作成するホストが所有している必要があります。
Do not assign drive letter or volume mount point	ディスクをWindowsで手動でマウントする場合に選択します。
LUN size	LUNサイズ (150MB以上) を指定します。 ドロップダウン リストで単位 (MB、GB、またはTB) を選択します。
Use thin provisioning for the volume hosting this LUN	LUNをシンプロビジョニングします。 シンプロビジョニングでは、ストレージ スペースが必要なときに必要な分だけ割り当てられるため、LUNは使用可能な最大容量まで効率的に拡張されます。 必要になるすべてのLUNストレージに対応できるだけの十分なスペースがボリュームにあることを確認してください。

プロパティ	説明
Choose partition type	GUIDパーティション テーブルの場合はGPTパーティション、 マスター ブート レコードの場合はMBRパーティションを選択します。 MBRパーティションをWindows Serverフェイルオーバー クラスタで使用した場合、 ミスアライメントが発生することがあります。  Unified Extensible Firmware Interface (UEFI) パーティション ディスクはサポートされていません。

8. [Map LUN]ページで、ホストのiSCSIイニシエータまたはFCイニシエータを選択します。

フィールド	操作
ホスト	クラスタ グループ名をダブルクリックし、ドロップダウン リストに表示されたクラスタに属するホストの中から、イニシエータに指定するホストを選択します。 このフィールドは、Windows Serverフェイルオーバー クラスタ内のホストでLUNを共有する場合にのみ表示されます。
Choose host initiator	ファイバー チャネル または iSCSI を選択し、ホスト上のイニシエーターを選択します。 FCでマルチパスI/O (MPIO) を使用する場合は、FCイニシエータを複数選択できます。

9. [Group Type]ページで、既存のigroupをLUNにマッピングするか新しいigroupを作成するかを指定します。

選択するオプション	状況
選択したイニシエータの新しい igroup を作成する	選択したイニシエータ用に新しいigroupを作成します。
Choose an existing igroup or specify a new igroup for selected initiators	選択したイニシエータ用に既存のigroupを指定するか、指定した名前で新しいigroupを作成します。 igroup 名 フィールドに igroup 名を入力します。既存のigroup名の最初の数文字を入力すると、残りの文字が自動的に入力されます。

10. 概要ページで選択内容を確認し、「完了」をクリックします。

SnapCenterにより、LUNが作成され、ホスト上の指定したドライブまたはドライブ パスに接続されま

す。

ディスクのサイズ変更

ストレージ システムのニーズの変化に応じて、ディスクのサイズを拡張または縮小することができます。

このタスクについて

- シンプロビジョニングLUNの場合、ONTAP LUNのジオメトリのサイズが最大サイズとして表示されます。
- シックプロビジョニングLUNの場合、拡張可能なサイズ（ボリューム内の使用可能なサイズ）が最大サイズとして表示されます。
- MBRパーティション方式を使用したLUNの場合、最大サイズは2TBです。
- GPTパーティション方式を使用したLUNの場合、ストレージ システムの最大サイズは16TBです。
- LUNのサイズを変更する前にSnapshotを作成しておくことを推奨します。
- LUNのサイズの変更前に作成されたSnapshotからLUNをリストアすると、SnapCenterによってLUNのサイズがSnapshotのサイズに自動的に変更されます。

リストア処理のあと、サイズ変更後にLUNに追加されたデータを、サイズ変更後に作成されたSnapshotからリストアする必要があります。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. [Host]ドロップダウン リストからホストを選択します。

ディスクのリストが表示されます。

4. サイズを変更するディスクを選択し、「サイズ変更」をクリックします。
5. [Resize Disk]ダイアログ ボックスで、スライダ ツールを使用してディスクの新しいサイズを指定するか、[Size]フィールドに新しいサイズを入力します。



サイズを手動で入力した場合は、入力後に[Size]フィールド以外の部分をクリックすると、[Shrink]ボタンまたは[Expand]ボタンが有効になります。また、[MB]、[GB]、または[TB]のいずれかをクリックして単位を指定する必要があります。

6. 入力内容に問題がなければ、必要に応じて 縮小 または 拡大 をクリックします。

SnapCenterによって、ディスクのサイズが変更されます。

ディスクの接続

[Connect Disk]ウィザードを使用して、既存のLUNをホストに接続したり、切断されたLUNを再接続したりできます。

開始する前に

- ストレージ システムでFCサービスまたはiSCSIサービスを開始しておく必要があります。
- iSCSIを使用している場合は、ストレージ システムとのiSCSIセッションを確立しておく必要があります。
- Windows Serverフェイルオーバー クラスタ内のホストで共有する場合を除き、LUNを複数のホストに接続することはできません。
- クラスタ共有ボリューム（CSV）を使用するWindows Serverフェイルオーバー クラスタ内のホスト間でLUNを共有する場合、クラスタ グループを所有するホストにディスクを接続する必要があります。
- Plug-in for Windowsをインストールする必要があるのは、ディスクを接続するホストだけです。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. *ホスト*ドロップダウンリストからホストを選択します。
4. *接続*をクリックします。

[Connect Disk]ウィザードが開きます。

5. [LUN Name]ページで、接続するLUNの情報を指定します。

フィールド	操作
Storage System	LUNのSVMを選択します。
LUN path	参照 をクリックして、LUN を含むボリュームの完全なパスを選択します。
LUN名	LUNの名前を入力します。
Cluster size	クラスタのLUNのブロック割り当てサイズを選択します。 クラスタのサイズは、オペレーティング システムおよびアプリケーションによって異なります。
LUN label	必要に応じて、LUNの説明を入力します。

6. [Disk Type]ページで、ディスク タイプを選択します。

選択するオプション	状況
Dedicated disk	LUNにアクセスできるホストは1つだけです。

選択するオプション	状況
共有ディスク	Windows Serverフェイルオーバー クラスタ内のホストでLUNを共有します。 ディスクはフェイルオーバー クラスタ内の1つのホストだけに接続します。
Cluster Shared Volume (CSV)	CSVを使用するWindows Serverフェイルオーバー クラスタ内のホストでLUNを共有します。 ディスクはクラスタ グループを所有するホストに接続する必要があります。

7. [Drive Properties]ページで、ドライブのプロパティを指定します。

プロパティ	説明
自動割り当て	システム ドライブに基づいて、SnapCenterで自動的にボリューム マウント ポイントを割り当てます。 たとえば、システム ドライブがC:であれば、C:ドライブにボリューム マウント ポイント (C:\scmnpt\l) が作成されます。自動割り当ては共有ディスクではサポートされません。
Assign drive letter	ドロップダウン リストで選択したドライブにディスクをマウントします。
Use volume mount point	フィールドで指定したドライブ パスにディスクをマウントします。 ボリューム マウント ポイントのルートは、ディスクを作成するホストが所有している必要があります。
Do not assign drive letter or volume mount point	ディスクをWindowsで手動でマウントする場合に選択します。

8. [Map LUN]ページで、ホストのiSCSIイニシエータまたはFCイニシエータを選択します。

フィールド	操作
ホスト	クラスタ グループ名をダブルクリックし、ドロップダウン リストに表示されたクラスタに属するホストの中から、イニシエータに指定するホストを選択します。 このフィールドは、Windows Serverフェイルオーバー クラスタ内のホストでLUNを共有する場合にのみ表示されます。
Choose host initiator	ファイバー チャネル または iSCSI を選択し、ホスト上のイニシエーターを選択します。 FCでMPIOを使用している場合は、FCイニシエーターを複数選択できます。

9. [Group Type]ページで、既存のigroupをLUNにマッピングするか新しいigroupを作成するかを指定します。

選択するオプション	状況
選択したイニシエータの新しい igroup を作成する	選択したイニシエータ用に新しいigroupを作成します。
Choose an existing igroup or specify a new igroup for selected initiators	選択したイニシエータ用に既存のigroupを指定するか、指定した名前で新しいigroupを作成します。 igroup 名 フィールドに igroup 名を入力します。既存のigroup名の最初の数文字を入力すると、残りの文字が自動的に入力されます。

10. 概要ページで選択内容を確認し、「完了」をクリックします。

SnapCenterにより、ホスト上の指定したドライブまたはドライブ パスにLUNが接続されます。

ディスクの切断

LUN の内容に影響を与えずにホストから LUN を切断できますが、1 つの例外があります: クローンを分割する前に切断すると、クローンの内容が失われます。

開始する前に

- LUNを使用しているアプリケーションがないことを確認します。
- LUNが監視ソフトウェアで監視されていないことを確認します。
- LUNが共有されている場合は、LUNからクラスタ リソースの依存関係を解除し、クラスタ内のすべてのノードの電源がオンで正常に動作しており、SnapCenterからアクセスできることを確認します。

このタスクについて

SnapCenterで作成したFlexCloneボリュームのLUNを切断した場合、そのボリュームに他のLUNが接続されて

いなければSnapCenterはボリュームも削除します。この場合、LUNが切断される前に、FlexCloneボリュームが削除される可能性があることを警告するメッセージがSnapCenterに表示されます。

FlexCloneボリュームが自動で削除されないようにするには、最後のLUNを切断する前にボリュームの名前を変更します。ボリュームの名前を変更する際は、最後の1文字だけでなく複数の文字を変更してください。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. *ホスト*ドロップダウンリストからホストを選択します。

ディスクのリストが表示されます。

4. 切断するディスクを選択し、「切断」をクリックします。
5. [ディスクの切断] ダイアログ ボックスで、[OK] をクリックします。

SnapCenterによってディスクが切断されます。

ディスクの削除

不要になったディスクは削除できます。削除したディスクは復元できません。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[ディスク] をクリックします。
3. *ホスト*ドロップダウンリストからホストを選択します。

ディスクのリストが表示されます。

4. 削除するディスクを選択し、「削除」をクリックします。
5. [ディスクの削除] ダイアログボックスで、[OK] をクリックします。

SnapCenterによってディスクが削除されます。

SMB共有の作成と管理

Storage Virtual Machine (SVM) 上にSMB3共有を設定するには、SnapCenterユーザ インターフェイスまたはPowerShellコマンドレットを使用できます。

ベスト プラクティス: コマンドレットを使用すると、SnapCenterに用意されているテンプレートを利用して共有構成を自動化できるため、コマンドレットの使用をお勧めします。

テンプレートには、ボリュームおよび共有の設定に関するベストプラクティスが組み込まれています。テンプレートは、SnapCenter Plug-ins Package for Windowsのインストール フォルダのTemplatesフォルダにあります。



必要に応じて、提供されるモデルに従って独自のテンプレートを作成することもできます。カスタム テンプレートを作成する場合は、コマンドレットのドキュメントでパラメータを確認してください。

SMB共有を作成する

SnapCenterの[Shares]ページを使用して、Storage Virtual Machine (SVM) にSMB3共有を作成できます。

SnapCenterを使用して SMB 共有上のデータベースをバックアップすることはできません。SMBでサポートされるのはプロビジョニングのみです。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[共有] をクリックします。
3. *ストレージ仮想マシン*ドロップダウンリストから SVM を選択します。
4. *新規*をクリックします。

[新しい共有] ダイアログが開きます。

5. [新しい共有] ダイアログで、共有を定義します。

フィールド	操作
説明	共有の説明を入力します。
シェア名	共有の名前を入力します（例：test_share）。 ここで入力した共有の名前はボリューム名としても使用されます。 共有名には次のルールが適用されます。 • UTF-8文字列である必要があります。 • 以下の文字を含めることはできません: 0x00から0x1Fまでの制御文字(両端を含む)、0x22(二重引用符)、および特殊文字 \ / [] : (vertical bar) < > + = ; , ?
パスを共有	• フィールドをクリックして、新しいファイル システム パス (例: /) を入力します。 • フィールドをダブルクリックし、既存のファイル システム パスのリストから選択します。

6. 入力内容に満足したら、「OK」をクリックします。

SnapCenter はSVM 上に SMB 共有を作成します。

SMB共有を削除する

不要になったSMB共有は削除できます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[共有] をクリックします。
3. [共有] ページで、[ストレージ仮想マシン] フィールドをクリックして、使用可能なストレージ仮想マシン (SVM) のリストを含むドロップダウンを表示し、削除する共有の SVM を選択します。
4. SVM 上の共有リストから、削除する共有を選択し、[削除] をクリックします。
5. [共有の削除] ダイアログボックスで、[OK] をクリックします。

SnapCenter はSVM から SMB 共有を削除します。

ストレージ システムでのスペースの再生

ファイルが削除または変更された場合、NTFSはLUN上の使用可能なスペースを追跡しますが、この情報はストレージ システムには報告されません。新たに解放されたブロックがストレージで空きスペースとしてマークされるようにするには、Plug-in for Windows ホストでスペース再生用のPowerShellコマンドレットを実行します。

リモートのプラグイン ホストでコマンドレットを実行する場合は、SnapCenterOpen-SMConnectionコマンドレットを実行してSnapCenter Serverへの接続を確立する必要があります。

開始する前に

- リストア処理を実行する前に必ずスペース再生プロセスを完了しておく必要があります。
- Windows Serverフェイルオーバー クラスタ内のホストでLUNを共有している場合は、クラスタ グループを所有するホストでスペース再生を実行する必要があります。
- ストレージのパフォーマンスを最適化するには、できるだけ頻繁にスペース再生を実行します。

NTFSファイルシステム全体がスキャンされたことを確認してください。

このタスクについて

- スペース再生には時間がかかり、CPUを大量に消費するため、通常はストレージ システムとWindowsホストがあまり使用されていない時間帯に実行することを推奨します。
- 使用可能なほぼすべてのスペースが再生されますが、100%ではありません。
- スペース再生の実行中にディスクのデフラグは実行しないでください。

再生プロセスの実行速度が低下する可能性があります。

ステップ

アプリケーション サーバのコマンド プロンプトで、次のPowerShellコマンドを入力します。

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

drive_pathは、LUNにマッピングされているドライブのパスです。

PowerShellコマンドレットを使用したストレージのプロビジョニング

SnapCenter GUI を使用してホストのプロビジョニングおよびスペース再利用ジョブを実行しない場合、PowerShell コマンドレットを使用できます。コマンドレットは直接使用できるほか、スクリプトに追加することもできます。

リモートのプラグイン ホストでコマンドレットを実行する場合は、SnapCenterのOpen-SMConnectionコマンドレットを実行してSnapCenter Serverへの接続を確立する必要があります。

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

SnapDrive for Windowsをサーバーから削除したためにSnapCenter PowerShellコマンドレットが機能しなくなった場合は、"[SnapDrive for Windows をアンインストールするとSnapCenterコマンドレットが壊れる](#)"。

VMware環境でのストレージのプロビジョニング

SnapCenter Plug-in for Microsoft Windowsは、VMware環境でのLUNの作成と管理やSnapshotの管理に使用できます。

サポートされるVMwareゲストOSプラットフォーム

- サポート対象バージョンのWindows Server
- Microsoftクラスタ構成

VMware上でサポートされるノードは、Microsoft iSCSI Software Initiatorを使用する場合は最大16、FCを使用する場合は最大2つです。

- RDM LUN

通常のRDMSでは、最大56のRDM LUNと4つのLSI Logic SCSIコントローラがサポートされます。VMware VM MSCSのボックスツースボックスのPlug-in for Windows構成では、最大42のRDM LUNと3つのLSI Logic SCSIコントローラがサポートされます。

VMware ParaVirtual SCSIコントローラがサポートされます。RDMディスクでは、256台のディスクがサポートされます。

サポートされているバージョンに関する最新情報については、"[NetApp Interoperability Matrix Tool](#)"。

VMware ESXiサーバ関連の制限事項

- 仮想マシンで構成されたMicrosoftクラスタにPlug-in for Windowsをインストールする場合、ESXiクレデンシャルは使用できません。

クラスタ化された仮想マシンにPlug-in for Windowsをインストールする場合、vCenterのクレデンシャルを使用する必要があります。

- クラスタ化されたすべてのノードで、同じクラスタ ディスクには同じ（仮想SCSIアダプタ上の）ターゲットIDを使用する必要があります。
- Plug-in for Windowsを使用せずにRDM LUNを作成した場合、プラグイン サービスを再起動し、作成したディスクを認識させる必要があります。
- VMwareゲストOSでiSCSIイニシエータとFCイニシエータを同時に使用することはできません。

SnapCenterのRDMの処理に必要な最小限のvCenter権限

ゲストOSでRDM処理を実行するには、ホストに対する次のvCenter権限が必要です。

- データストア: ファイルの削除
- ホスト: 構成 > ストレージパーティション構成
- 仮想マシン: 構成

これらの権限を、仮想センター サーバ レベルのロールに割り当てる必要があります。これらの権限を割り当てたロールをroot権限を持たないユーザに割り当てることはできません。

これらの権限を割り当てたら、ゲストOSにPlug-in for Windowsをインストールできます。

MicrosoftクラスタのFC RDM LUNの管理

Plug-in for Windowsを使用して、FC RDM LUNを使用するMicrosoftクラスタを管理するには、プラグインの外部で共有RDMクォーラムと共有ストレージを作成し、クラスタ内の仮想マシンにディスクを追加しておく必要があります。

ESXi 5.5以降、ESXのiSCSIハードウェアやFCoEハードウェアを使用したMicrosoftクラスタの管理も可能となりました。Plug-in for Windowsでは、設定作業なしでMicrosoftクラスタがサポートされます。

要件

Plug-in for Windowsでは、一定の構成要件を満たしていれば、2つの異なるESXまたはESXiサーバに属する2台の仮想マシン上のFC RDM LUNを使用したMicrosoftクラスタ（筐体間クラスタ）がサポートされます。

- 各仮想マシン（VM）が同じバージョンのWindows Serverを実行している必要があります。
- 各VMware親ホストのESX / ESXiサーバのバージョンが同じである必要があります。
- 各親ホストに少なくとも2つのネットワーク アダプタが必要です。
- 2台のESX / ESXiサーバ間でVMware Virtual Machine File System（VMFS）データストアを少なくとも1つ共有している必要があります。
- VMwareでは、共有データストアをFC SANで作成することを推奨しています。

共有データストアは、必要に応じてiSCSIで作成することもできます。

- 共有RDM LUNが物理互換モードである必要があります。
- 共有RDM LUNは、Plug-in for Windowsの外部で手動で作成する必要があります。

共有ストレージに仮想ディスクを使用することはできません。

- クラスタ内の各仮想マシンに、SCSIコントローラが物理互換モードで構成されている必要があります。

Windows Server 2008 R2の場合、各仮想マシンにLSI Logic SAS SCSIコントローラを構成する必要があります。LSI Logic SASタイプのコントローラが1台しかなく、すでにC:ドライブに接続されている場合、そのコントローラを共有LUNで使用することはできません。

準仮想化タイプのSCSIコントローラはVMware Microsoftクラスタではサポートされていません。



物理互換モードの仮想マシン上の共有 LUN に SCSI コントローラを追加する場合は、VMware Infrastructure Client で 新しいディスクの作成 オプションではなく、**Raw** デバイス マッピング (RDM) オプションを選択する必要があります。

- Microsoft仮想マシン クラスタをVMwareクラスタに含めることはできません。
- Microsoftクラスタに属する仮想マシンにPlug-in for Windowsをインストールする場合は、ESXまたはESXiのクレデンシャルではなくvCenterのクレデンシャルを使用する必要があります。
- Plug-in for Windowsでは、複数のホストのイニシエータを含むigroupを作成することはできません。

共有クラスタ ディスクとして使用するRDM LUNを作成する前に、すべてのESXiホストのイニシエータを含むigroupをストレージ コントローラ上に作成しておく必要があります。

- ESXi 5.0では、FCイニシエータを使用してRDM LUNを作成します。

RDM LUNを作成すると、ALUAでイニシエータ グループが作成されます。

制限事項

Plug-in for Windowsでは、異なるESXサーバまたはESXiサーバに属する異なる仮想マシン上のFC / iSCSI RDM LUNを使用するMicrosoftクラスタがサポートされます。



この機能は、ESX 5.5iよりも前のリリースではサポートされていません。

- Plug-in for Windowsでは、ESX iSCSIおよびNFSデータストア上のクラスタはサポートされません。
- Plug-in for Windowsでは、クラスタ環境でのイニシエータの混在はサポートされません。

イニシエータはFCとMicrosoft iSCSIのどちらか一方にする必要があります。

- ESX iSCSIイニシエータとHBAはMicrosoftクラスタ内の共有ディスクではサポートされません。
- Plug-in for Windowsでは、Microsoftクラスタに属する仮想マシンのvMotionによる移行はサポートされません。
- Plug-in for Windowsでは、Microsoftクラスタ内の仮想マシンでのMPIOはサポートされません。

共有FC RDM LUNの作成

FC RDM LUNを使用してMicrosoftクラスタ内のノード間でストレージを共有する場合、事前に共有クォーラム ディスクと共有ストレージ ディスクを作成し、それらをクラスタ内の両方の仮想マシンに追加しておく必要があります。

共有ディスクの作成にPlug-in for Windowsは使用しません。共有LUNを作成し、クラスタ内の各仮想マシンに追加する必要があります。詳細については、["物理ホスト間で仮想マシンをクラスタ化する"](#)。

SnapCenter Standardコントローラベース ライセンスの追加

FAS、AFF、またはASAストレージ コントローラを使用している場合は、SnapCenter Standard コントローラ ベースのライセンスが必要です。

コントローラベース ライセンスには次のような特徴があります。

- SnapCenter Standardライセンスは、Premium BundleまたはFlash Bundleに含まれています（Base Packには含まれていません）。
- ストレージ容量に制限はありません。
- ONTAP System Manager またはONTAP CLI を使用して、FAS、AFF、またはASAストレージ コントローラに直接追加されます。



SnapCenterコントローラベースのライセンスについては、SnapCenterユーザー インターフェイスにライセンス情報を入力しません。

- コントローラのシリアル番号に紐付けられます。

必要なライセンスについては、以下を参照してください。["SnapCenterのライセンス"](#)。

ステップ1: SnapManager Suiteライセンスがインストールされているかどうかを確認する

SnapCenterユーザー インターフェイスを使用して、SnapManager Suite ライセンスがFAS、AFF、またはASAプライマリ ストレージ システムにインストールされているかどうかを確認し、ライセンスが必要なシステムを特定できます。SnapManager Suiteライセンスは、プライマリ ストレージ システム上のFAS、AFF、およびASA SVM / クラスタにのみ適用されます。



コントローラにすでにSnapManager Suite ライセンスがある場合、SnapCenter は標準コントローラベースのライセンス権限を自動的に提供します。SnapManager SuiteライセンスとSnapCenter Standardコントローラベース ライセンスは同じライセンスを表しています。

手順

1. 左側のナビゲーション ペインで、*ストレージ システム*を選択します。
2. [ストレージ システム] ページの [タイプ] ドロップダウンから、追加されたすべての SVM またはクラスターを表示するかどうかを選択します。
 - 追加されたすべての SVM を表示するには、* ONTAP SVM* を選択します。
 - 追加されたすべてのクラスターを表示するには、* ONTAPクラスター* を選択します。

クラスタ名を選択すると、そのクラスタに含まれるすべてのSVMが[Storage Virtual Machine]セクションに表示されます。

3. [ストレージ接続]リストの[コントローラ ライセンス]列を確認します。

[Controller License]列には、次のステータスが表示されます。

◦



SnapManager Suite ライセンスがFAS、AFF、またはASAプライマリ ストレージ システムにインストールされていることを示します。

-  SnapManager Suite ライセンスがFAS、AFF、またはASAプライマリ ストレージ システムにインストールされていないことを示します。
- [Not Applicable]は、ストレージ コントローラがAmazon FSx for NetApp ONTAP、Cloud Volumes ONTAP、ONTAP Select、またはセカンダリ ストレージ プラットフォーム上にあるため、SnapManager Suiteライセンスが適用されないことを示します。

ステップ2: コントローラにインストールされているライセンスを識別する

ONTAPコマンドラインを使用して、コントローラにインストールされているすべてのライセンスを表示できます。FAS、AFF、またはASAシステムのクラスタ管理者である必要があります。



コントローラには、SnapCenter Standard コントローラ ベースのライセンスが SnapManagerSuite ライセンスとして表示されます。

手順

1. ONTAPコマンドラインを使用してNetAppコントローラにログインします。
2. license show コマンドを入力し、出力を表示して SnapManagerSuite ライセンスがインストールされているかどうかを確認します。

出力例

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package          Type      Description          Expiration
-----
Base             site     Cluster Base License -

Serial Number: 1-81-000000000000000000000000xx
Owner: cluster1-01
Package          Type      Description          Expiration
-----
NFS              license   NFS License         -
CIFS             license   CIFS License        -
iSCSI            license   iSCSI License       -
FCP              license   FCP License         -
SnapRestore      license   SnapRestore License -
SnapMirror       license   SnapMirror License  -
FlexClone        license   FlexClone License   -
SnapVault        license   SnapVault License   -
SnapManagerSuite license   SnapManagerSuite License -
```

この例では、SnapManager Suiteライセンスがインストールされているため、SnapCenterライセンスを設定する必要はありません。

ステップ3: コントローラーのシリアル番号を取得する

ONTAPコマンドラインを使用してコントローラのシリアル番号を取得します。コントローラベースのライセンスのシリアル番号を取得するには、FAS、AFF、またはASAシステムのクラスタ管理者である必要があります。

手順

1. ONTAPコマンドラインを使用してコントローラにログインします。
2. `system show -instance` コマンドを入力し、その出力でコントローラのシリアル番号を確認します。

```
cluster1::> system show -instance
```

```
Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
```

```
Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. シリアル番号をメモします。

ステップ4: コントローラベースのライセンスのシリアル番号を取得する

FAS、ASA、またはAFFストレージを使用している場合は、ONTAPコマンドラインを使用してインストールする前に、NetAppサポート サイトからSnapCenterコントローラベースのライセンスを取得できます。

開始する前に

- NetAppサポート サイトの有効なログイン クレデンシャルが必要です。

有効な資格情報を入力しない場合は、検索に対して情報が返されません。

- コントローラのシリアル番号が必要です。

手順

1. ログイン ["NetAppサポート サイト"](#)。
2. システム > ソフトウェア ライセンス に移動します。
3. [選択基準] 領域で、[シリアル番号] (ユニットの背面にあります) が選択されていることを確認し、コントローラのシリアル番号を入力して、[Go!] を選択します。



Software Licenses

Selection Criteria

Choose a method by which to search

▶ Serial Number (located on back of unit) ▾ Enter Value: Go!

Enter the Cluster Serial Number value without dashes.

- OR -

▶ Show Me All: Serial Numbers with Licenses ▾ For Company: Go!

指定したコントローラのライセンスのリストが表示されます。

4. SnapCenter StandardまたはSnapManager Suiteのライセンスをメモします。

ステップ5: コントローラベースのライセンスを追加する

FAS、AFF、またはASAシステムを使用していて、SnapCenter StandardまたはSnapManager Suiteのライセンスがある場合は、ONTAPコマンドラインを使用してSnapCenterコントローラベース ライセンスを追加できます。

開始する前に

- FAS、AFF、またはASAシステムのクラスタ管理者である必要があります。
- SnapCenter StandardまたはSnapManager Suiteのライセンスが必要です。

タスク概要

FAS、AFF、またはASAストレージにSnapCenterの試用版をインストールしたい場合は、Premium Bundleの評価版ライセンスを入手してコントローラにインストールできます。

SnapCenterの試用版をインストールする場合は、営業担当者からPremium Bundleの評価版ライセンスを入手してコントローラにインストールする必要があります。

手順

1. ONTAPコマンドラインを使用してNetAppクラスタにログインします。
2. SnapManager Suiteライセンス キーを追加します。

```
system license add -license-code license_key
```

このコマンドは、admin権限レベルで使用できます。

3. SnapManager Suiteライセンスがインストールされたことを確認します。

```
license show
```

ステップ6: 試用ライセンスを削除する

コントローラベースのSnapCenter Standard ライセンスを使用しており、容量ベースの試用ライセンス (シリアル番号が「50」で終わる) を削除する必要がある場合は、MySQL コマンドを使用して試用ライセンスを手動で削除する必要があります。試用ライセンスは、SnapCenterユーザー インターフェイスを使用して削除することはできません。



試用版ライセンスを手動で削除する必要があるのは、SnapCenter Standardコントローラベースライセンスを使用している場合のみです。

手順

1. SnapCenter Serverで、PowerShellウィンドウを開いてMySQLパスワードをリセットします。
 - a. Open-SmConnection コマンドレットを実行して、SnapCenterAdmin アカウントのSnapCenter Serverとの接続を確立します。
 - b. Set-SmRepositoryPasswordを実行してMySQLパスワードをリセットします。

コマンドレットの詳細については、以下を参照してください。 ["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

2. コマンド プロンプトを開き、mysql -u root -pを実行してMySQLにログインします。

パスワードの入力を求められます。パスワードのリセット時に指定したクレデンシャルを入力します。

3. データベースから試用版ライセンスを削除します。

```
use nsm;DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
```

高可用性の設定

SnapCenterサーバを高可用性向けに構成する

Windows または Linux 上で実行されているSnapCenterで高可用性 (HA) をサポートするには、F5 ロード バランサをインストールできます。F5により、SnapCenter Serverは、同じ場所にある最大2つのホストでアクティブ / パッシブ構成をサポートできます。SnapCenterでF5ロード バランサを使用するには、SnapCenter Serverを設定し、F5 ロード バランサを設定する必要があります。

ネットワーク負荷分散 (NLB) を構成して、SnapCenter の高可用性を設定することもできます。高可用性を実現するには、SnapCenterインストールの外部で NLB を手動で構成する必要があります。

クラウド環境では、Amazon Web Services (AWS) Elastic Load Balancing (ELB) と Azure ロードバランサーのいずれかを使用して高可用性を構成できます。

F5を使用した高可用性の設定

F5ロードバランサを使用して高可用性を実現するSnapCenterサーバの構成手順については、以下を参照してください。"[F5 ロードバランサを使用してSnapCenterサーバを高可用性に構成する方法](#)"。

次のコマンドレットを使用してF5クラスタを追加および削除するには、（SnapCenterAdminロールが割り当てられた）SnapCenter Serverのローカル管理者グループのメンバーである必要があります。

- Add-SmServerCluster
- Add-SmServer
- Remove-SmServerCluster

```
https://docs.netapp.com/us-en/snapcenter-  
cmdlets/index.html["SnapCenterソフトウェア コマンドレット リファレンス  
ガイド"^] 。
```

追加情報

- SnapCenterをインストールして高可用性を実現するための設定を行ったあとで、F5クラスタのIPを指すようにSnapCenterデスクトップのショートカットを編集します。
- SnapCenter Server間のフェイルオーバーが発生し、SnapCenterの既存のセッションも存在する場合は、ブラウザを閉じてからSnapCenterに再度ログオンする必要があります。
- ロード バランサ セットアップ (NLB または F5) で、NLB または F5 ホストによって部分的に解決されるホストを追加し、SnapCenterホストがこのホストにアクセスできない場合、SnapCenterホスト ページでは、ホストのダウン状態と実行状態が頻繁に切り替わります。この問題を解決するには、両方のSnapCenterホストがNLB または F5 ホストでホストを解決できることを確認する必要があります。
- MFA 設定用のSnapCenterコマンドは、すべてのホストで実行する必要があります。証明書利用者の設定は、F5クラスタの詳細を使用してActive Directoryフェデレーション サービス (AD FS) サーバで行う必要があります。MFA を有効にすると、ホスト レベルのSnapCenter UI アクセスがブロックされます。
- フェイルオーバー中、監査ログ設定は2番目のホストに反映されません。したがって、F5 パッシブホストがアクティブになったときに、監査ログ設定を手動で繰り返す必要があります。

ネットワーク負荷分散 (NLB) を使用して高可用性を構成する

ネットワーク負荷分散 (NLB) を構成して、SnapCenter の高可用性を設定できます。高可用性を実現するには、SnapCenterインストールの外部でNLBを手動で構成する必要があります。

SnapCenterでネットワーク負荷分散 (NLB) を構成する方法については、以下を参照してください。"[SnapCenterでNLBを構成する方法](#)"。

AWS Elastic Load Balancing (ELB) を使用して高可用性を構成する

2 台のSnapCenterサーバを別々のアベイラビリティゾーン (AZ) に設定し、自動フェイルオーバーを構成することで、Amazon Web Services (AWS) で高可用性SnapCenter環境を構成できます。アーキテクチャには、仮想プライベート IP アドレス、ルーティング テーブル、アクティブおよびスタンバイMySQL データベース間の同期が含まれます。

手順

1. AWS で仮想プライベートオーバーレイ IP を構成します。詳細については、["仮想プライベートオーバーレイIPを構成する"](#)。
2. Windowsホストを準備する
 - a. IPv4 を IPv6 よりも優先させる:
 - 場所: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
 - キー: DisabledComponents
 - タイプ: REG_DWORD
 - 値: 0x20
 - b. 完全修飾ドメイン名が DNS またはローカル ホスト構成を介して IPv4 アドレスに解決できることを確認します。
 - c. システム プロキシが構成されていないことを確認してください。
 - d. Active Directory のないセットアップを使用し、サーバーが同じドメインにない場合は、両方の Windows Server で管理者パスワードが同じであることを確認します。
 - e. 両方の Windows サーバーに仮想 IP を追加します。
3. SnapCenterクラスターを作成します。
 - a. Powershell を起動し、SnapCenterに接続します。

```
Open-SmConnection
```
 - b. クラスターを作成します。

```
Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator
```
 - c. セカンダリ サーバーを追加します。

```
Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator
```
 - d. 高可用性の詳細を取得します。

```
Get-SmServerConfig
```
4. AWS CloudWatch によって監視されている仮想プライベート IP エンドポイントが使用できなくなった場合にルーティング テーブルを調整する Lambda 関数を作成します。詳細については、["Lambda関数を作成する"](#)。
5. SnapCenterエンドポイントの可用性を監視するために、CloudWatch でモニターを作成します。エンドポイントに到達できない場合に Lambda 関数をトリガーするようにアラームが設定されています。Lambda 関数はルーティング テーブルを調整して、トラフィックをアクティブなSnapCenterサーバーにリダイレクトします。詳細については、["合成カナリアを作成する"](#)。
6. CloudWatch モニタリングの代替としてステップ関数を使用してワークフローを実装し、フェイルオーバー時間を短縮します。ワークフローには、SnapCenter URL をテストするための Lambda プローブ関数、失敗数を保存するための DynamoDB テーブル、および Step Function 自体が含まれています。
 - a. SnapCenter URL を調査するには、Lambda 関数を使用します。詳細については、["Lambda関数を作成する"](#)。
 - b. 2 回の Step Function 反復間の失敗回数を保存するための DynamoDB テーブルを作成します。詳細については、["DynamoDBテーブルを使い始める"](#)。

- c. ステップ関数を作成します。詳細については、["Step Function ドキュメント"](#)。
- d. 単一のステップをテストします。
- e. 完全な機能をテストします。
- f. IAM ロールを作成し、Lambda 関数を実行できるように権限を調整します。
- g. Step Function をトリガーするスケジュールを作成します。詳細については、["Amazon EventBridge Scheduler を使用して Step Functions を開始する"](#)。

Azure ロード バランサーを使用して高可用性を構成する

Azure ロード バランサーを使用して、高可用性SnapCenter環境を構成できます。

手順

1. Azure ポータルを使用してスケール セット内に仮想マシンを作成します。Azure 仮想マシン スケール セットを使用すると、負荷分散された仮想マシンのグループを作成して管理できます。仮想マシン インスタンスの数は、需要または定義されたスケジュールに応じて自動的に増加または減少します。詳細については、["Azure ポータルを使用してスケール セットに仮想マシンを作成する"](#)。
2. 仮想マシンを構成した後、VM セット内の各仮想マシンにログインし、両方のノードにSnapCenter Server をインストールします。
3. ホスト 1 にクラスターを作成します。

```
Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>
```
4. セカンダリ サーバーを追加します。

```
Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>
```
5. 高可用性の詳細を取得します。

```
Get-SmServerConfig
```
6. 必要に応じて、セカンダリ ホストを再構築します。

```
Set-SmRepositoryConfig -RebuildSlave -Verbose
```
7. 2 番目のホストにフェイルオーバーします。

```
Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose
```

== 高可用性のために NLB から F5 に切り替える

SnapCenterのHA構成を、ネットワーク負荷分散（NLB）からF5ロード バランサに変更できます。

手順

1. F5 を使用して、高可用性を実現するSnapCenterサーバーを構成します。["詳細情報"](#)。
2. SnapCenter Serverホストで、PowerShellを起動します。
3. Open-SmConnectionコマンドレットを使用してセッションを開始し、クレデンシャルを入力します。
4. Update-SmServerClusterコマンドレットを使用して、F5クラスターのIPアドレスを指すようにSnapCenter Serverを更新します。

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実

行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

SnapCenter MySQLリポジトリの高可用性

MySQL Serverの機能であるMySQLレプリケーションを使用すると、MySQLデータベース サーバ（マスター）から別のMySQLデータベース サーバ（スレーブ）へ、データをレプリケートできます。SnapCenterでは、ネットワーク負荷分散（NLB）が有効な2つのノード間でのみ、高可用性実現のためにMySQLレプリケーションをサポートしています。

SnapCenterは、マスター リポジトリに対して読み取りまたは書き込みの処理を実行し、マスター リポジトリで障害が発生した場合はスレーブ リポジトリへ接続をルーティングします。この場合、スレーブ リポジトリがマスター リポジトリになります。SnapCenterでは逆方向のレプリケーションもサポートされており、これはフェイルオーバー時にのみ有効になります。

MySQL高可用性（HA）機能を使用する場合は、1つ目のノードにネットワーク ロード バランサ（NLB）を設定する必要があります。MySQLリポジトリは、インストール中にこのノードにインストールされます。2つ目のノードにSnapCenterをインストールするときは、1つ目のノードのF5に追加して、2つ目のノードにMySQLリポジトリのコピーを作成する必要があります。

SnapCenter は、MySQL レプリケーションを管理するための *Get-SmRepositoryConfig* および *Set-SmRepositoryConfig* PowerShell コマンドレットを提供します。

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

MySQL HA機能に関連する次の制限事項を理解しておく必要があります。

- NLBとMySQL HAがサポートされるのは、2つのノードまでです。
- SnapCenterスタンドアロン インストールからNLBインストールまたはその逆の切り替えや、MySQLスタンドアロン セットアップからMySQL HAへの切り替えはサポートされていません。
- スレーブ リポジトリのデータがマスター リポジトリのデータと同期されていない場合、自動フェイルオーバーはサポートされません。

Set-SmRepositoryConfig コマンドレットを使用して強制フェールオーバーを開始できます。

- フェイルオーバーが開始されると、実行中のジョブが失敗する場合があります。

MySQL ServerまたはSnapCenter Serverがダウンしたためにフェイルオーバーが発生した場合、実行中のすべてのジョブが失敗する可能性があります。2つ目のノードへのフェイルオーバー後、後続のすべてのジョブは正常に実行されます。

高可用性の構成については、以下を参照してください。"[SnapCenterでNLBとARRを構成する方法](#)"。

ロールベース アクセス制御（RBAC）の設定

ロールの作成

既存のSnapCenterロールを使用するだけでなく、独自のロールを作成し、権限をカスタマイズすることもできます。

独自のロールを作成するには、「SnapCenterAdmin」ロールとしてログインする必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. 設定ページで、「ロール」 をクリックします。
3. クリック .
4. 新しいロールの名前と説明を指定します。



ユーザー名とグループ名には、スペース ()、ハイフン (-)、アンダースコア (_)、コロン (:) の特殊文字のみを使用できます。

5. このロールのすべてのメンバーが他のメンバーのオブジェクトを表示できる を選択すると、ロールの他のメンバーは、リソース リストを更新した後にボリュームやホストなどのリソースを表示できるようになります。

このロールのメンバーに他のメンバーが割り当てられているオブジェクトを表示しない場合は、このオプションをオフにします。



このオプションを有効にすると、オブジェクトまたはリソースを作成したユーザと同じロールに属しているユーザにオブジェクトまたはリソースへのアクセスを割り当てる必要がなくなります。

6. 「権限」 ページで、ロールに割り当てる権限を選択するか、「すべて選択」 をクリックしてロールにすべての権限を付与します。
7. *送信* をクリックします。

セキュリティ ログイン コマンドを使用して**NetApp ONTAP RBAC** ロールを追加する

ストレージ システムでクラスタ化されたONTAP を実行している場合は、セキュリティ ログイン コマンドを使用してNetApp ONTAP RBAC ロールを追加できます。

開始する前に

- 実行するタスク (1 つまたは複数) と、それらのタスクを実行するために必要な権限を特定します。
- コマンドおよびコマンド ディレクトリ、またはそのいずれかに権限を付与します。

コマンドおよびコマンド ディレクトリのアクセス権限には、フルアクセスと読み取り専用の2つのレベルがあります。

フルアクセス権限は、常に最初に付与する必要があります。

- ユーザにロールを割り当てます。
- SnapCenterプラグインがクラスタ全体の Cluster Administrator IP に接続されているか、クラスタ内の

SVM に直接接続されているかに応じて構成を識別します。

タスク概要

ストレージ システムでのこれらのロールの構成を簡素化するには、NetAppコミュニティ フォーラムに掲載されているNetApp ONTAPツール用の RBAC User Creator を使用できます。

このツールは、ONTAPの権限の適切な設定を自動的に処理します。たとえば、NetApp ONTAPツールの RBAC User Creator は、すべてのアクセス権限が最初に表示されるように、権限を正しい順序で自動的に追加します。読み取り専用権限を最初に追加し、次にフルアクセス権限を追加すると、ONTAPはフルアクセス権限を重複するものとしてマーキングし、無視します。



後でSnapCenterまたはONTAPをアップグレードする場合は、NetApp ONTAPツールの RBAC User Creator を再実行して、以前に作成したユーザー ロールを更新する必要があります。前のバージョンのSnapCenterまたはONTAP用に作成したユーザー ロールは、アップグレード後のバージョンでは正常に機能しません。ツールを再度実行すると、アップグレードが自動的に処理されます。ロールを再作成する必要はありません。

ONTAP RBACロールの設定の詳細については、["ONTAP 9 管理者認証および RBAC パワーガイド"](#)。

手順

1. ストレージ システムで、次のコマンドを入力して新しいロールを作成します。

```
security login role create <role_name\> -cmddirname "command" -access all  
-vserver <svm_name\>
```

- svm_nameには、SVMの名前を指定します。これを空白のままにした場合、デフォルトでクラスタ管理者が指定されます。
- role_nameは、ロールに指定する名前です。
- commandは、ONTAPの機能です。



このコマンドは、権限ごとに実行する必要があります。フルアクセス コマンドは、読み取り専用コマンドの前にリストする必要があります。

権限のリストについては、以下を参照してください。["ロールの作成と権限の割り当てのためのONTAP CLIコマンド"](#)。

2. 次のコマンドを入力して、ユーザ名を作成します。

```
security login create -username <user_name\> -application ontapi -authmethod  
<password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment  
"user_description"
```

- user_nameは、作成するユーザの名前です。
- <password> はあなたのパスワードです。パスワードを指定しないと、パスワードの入力を求めるプロンプトが表示されます。
- svm_nameには、SVMの名前を指定します。

3. 次のコマンドを入力して、ユーザにロールを割り当てます。

```
security login modify username <user_name\> -vserver <svm_name\> -role
```



```
<role_name\> -application ontapi -application console -authmethod <password\>
```

- <user_name> は、手順 2 で作成したユーザーの名前です。このコマンドでは、ロールに関連付けるユーザーを変更できます。
- <svm_name> は SVM の名前です。
- <role_name> は、手順 1 で作成したロールの名前です。
- <password> はあなたのパスワードです。パスワードを指定しないと、パスワードの入力を求めるプロンプトが表示されます。

4. 次のコマンドを入力して、ユーザが正しく作成されたことを確認します。

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

user_nameは、手順3で作成したユーザ名です。

最小権限でのSVMロールの作成

ONTAP内の新しいSVMユーザにロールを作成する場合、複数のONTAP CLIコマンドを実行する必要があります。ONTAP内のSVMをSnapCenterで使用するよう設定し、vsadminロールを使用したくない場合、このロールが必要です。

手順

1. ストレージ システムで、ロールを作成してすべての権限を割り当てます。

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>  
-cmddirname <permission\>
```



このコマンドは、権限ごとに実行する必要があります。

2. ユーザを作成してロールを割り当てます。

```
security login create -user <user_name\> -vserver <svm_name\> -application  
ontapi -authmethod password -role <SVM_Role_Name\>
```

3. ユーザのロックを解除します。

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

SVMロールの作成と権限の割り当てのためのONTAP CLIコマンド

SVMロールを作成して権限を割り当てるために実行する必要があるONTAP CLIコマンドがあります。

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname

```

"job history show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "job show" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "job stop" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "lun" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun igroup add" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun igroup create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun igroup delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun igroup rename" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun igroup show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun mapping add-reporting-nodes" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "lun mapping create" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun mapping delete" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun mapping remove-reporting-nodes" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun mapping show" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun modify" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun move-in-volume" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun offline" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun online" -access all
• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun resize" -access all

```

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```

"volume file show-disk-usage" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume modify" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume offline" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume online" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree delete" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree modify" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume restrict" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot delete" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot modify" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "volume snapshot modify-snaplock-expiry-time" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot rename" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot restore" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot restore-file" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot show-delta" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume unmount" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver cifs share create" -access all

```

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname

```
"nvme subsystem show" -access all
```

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all

ASA r2 システムの SVM ロールを作成する

ASA r2 システムで新しい SVM ユーザーのロールを作成するには、いくつかのONTAP CLI コマンドを実行する必要があります。このロールは、ASA r2 システムで SVM をSnapCenterで使用するように構成し、vsadmin ロールを使用しない場合に必要です。

手順

1. ストレージ システムで、ロールを作成してすべての権限を割り当てます。

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>  
-cmddirname <permission\>
```



このコマンドは、権限ごとに実行する必要があります。

2. ユーザを作成してロールを割り当てます。

```
security login create -user <user_name\> -vserver <svm_name\> -application  
http -authmethod password -role <SVM_Role_Name\>
```

3. ユーザのロックを解除します。

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

SVMロールの作成と権限の割り当てのためのONTAP CLIコマンド

SVMロールを作成して権限を割り当てるために実行する必要があるONTAP CLIコマンドがあります。

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"lun show" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```

"vserver cifs share show" -access all

```

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "consistency-group" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all
- security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name
- security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name

最小権限でのONTAPクラスタ ロールの作成

最小権限でONTAPクラスタ ロールを作成し、ONTAP adminロールを使用しなくてもSnapCenterで処理を実行できるようにする必要があります。いくつかのONTAP CLIコマンドを実行して、ONTAPクラスタ ロールを作成し、最小権限を割り当てることができます。

手順

1. ストレージ システムで、ロールを作成してすべての権限を割り当てます。

```
security login role create -vserver <cluster_name>- role <role_name>-
-cmddirname <permission>
```



このコマンドは、権限ごとに実行する必要があります。

2. ユーザを作成してロールを割り当てます。

```
security login create -user <user_name> -vserver <cluster_name> -application
ontapi http -authmethod password -role <role_name>
```

3. ユーザのロックを解除します。

```
security login unlock -user <user_name> -vserver <cluster_name>
```

クラスタ ロールを作成して権限を割り当てるために実行する必要があるONTAP CLIコマンドがあります。

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all`

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"nvme subsystem modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem host" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem controller" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "security login" -access readonly
• security login role create -role Role_Name -cmddirname "snapmirror create"
  -vserver Cluster_name -access all
• security login role create -role Role_Name -cmddirname "snapmirror list-
  destinations" -vserver Cluster_name -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy add-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy modify-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy remove-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror restore" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror show-history" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"volume snapshot modify-snaplock-expiry-time" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume offline" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume online" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume restrict" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot promote" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot rename" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot restore" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot restore-file" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot show-delta" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume unmount" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs create" -access all

```


- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all

ASA r2システム用のONTAPクラスタロールを作成する

最小権限でONTAPクラスタ ロールを作成し、ONTAP adminロールを使用しないで

もSnapCenterで処理を実行できるようにする必要があります。いくつかのONTAP CLI コマンドを実行して、ONTAPクラスタ ロールを作成し、最小権限を割り当てることができます。

手順

1. ストレージ システムで、ロールを作成してすべての権限を割り当てます。

```
security login role create -vserver <cluster_name\>- role <role_name\>  
-cmddirname <permission\>
```



このコマンドは、権限ごとに実行する必要があります。

2. ユーザを作成してロールを割り当てます。

```
security login create -user <user_name\> -vserver <cluster_name\> -application  
http -authmethod password -role <role_name\>
```

3. ユーザのロックを解除します。

```
security login unlock -user <user_name\> -vserver <cluster_name\>
```

クラスタ ロールの作成と権限の割り当てのための**ONTAP CLI**コマンド

クラスタ ロールを作成して権限を割り当てるために実行する必要のあるONTAP CLIコマンドがあります。

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"lun serial" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface create" -access readonly

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface delete" -access readonly

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface modify" -access readonly

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface show" -access readonly

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem map" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem host" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem controller" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "security login" -access readonly

• security login role create -role Role_Name -cmddirname "snapmirror create"
  -vserver Cluster_name -access all

• security login role create -role Role_Name -cmddirname "snapmirror list-
  destinations" -vserver Cluster_name -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy add-rule" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"volume clone create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone split start" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone split stop" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume destroy" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume file clone create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume file show-disk-usage" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot modify-snaplock-expiry-time" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume offline" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume online" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume restrict" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot modify" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"vserver export-policy rule create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver iscsi connection show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "storage-unit show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "consistency-group" show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror protect" show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume delete" show" -access all

```

ユーザまたはグループの追加と、ロールとアセットの割り当て

SnapCenterユーザのロールベース アクセス制御を設定するには、ユーザまたはグループを追加してロールを割り当てます。ロールに基づいて、SnapCenterユーザがアクセスできるオプションが決まります。

開始する前に

- 「SnapCenterAdmin」ロールでログインする必要があります。
- オペレーティング システムまたはデータベースのActive Directoryにユーザまたはグループのアカウントを作成しておく必要があります。SnapCenterでこれらのアカウントを作成することはできません。



ユーザー名とグループ名には、スペース ()、ハイフン (-)、アンダースコア (_)、コロン (:) の特殊文字のみを含めることができます。

- SnapCenterには、事前定義されたロールが複数あります。

これらのロールをユーザに割り当てるか、新しいロールを作成できます。

- SnapCenter RBACに追加するADユーザとADグループには、Active DirectoryのUsersコンテナとComputersコンテナに対する読み取り権限が必要です。

- まず適切な権限を含むロールをユーザまたはグループに割り当ててから、SnapCenterのアセット（ホストやストレージ接続など）へのアクセスをそのユーザに割り当てる必要があります。

これにより、ユーザは、自身に割り当てられたアセットに対して、権限のある処理を実行できるようになります。

- RBACの権限と効率性を活用するためには、いずれかの時点でユーザまたはグループにロールを割り当てる必要があります。
- ユーザまたはグループの作成時に、ホスト、リソース グループ、ポリシー、ストレージ接続、プラグイン、クレデンシャルなどのアセットをユーザに割り当てることができます。
- 特定の処理を実行するためにユーザに割り当てる必要がある最小アセットは次のとおりです。

処理	割り当てるアセット
リソースの保護	ホスト、ポリシー
バックアップ	ホスト、リソース グループ、ポリシー
リストア	ホスト、リソース グループ
クローン	ホスト、リソース グループ、ポリシー
クローンのライフサイクル	ホスト
リソース グループの作成	ホスト

- WindowsクラスタまたはDAG（Exchange Serverデータベース可用性グループ）アセットに新しいノードが追加され、そのノードがユーザに割り当てられた場合は、アセットをユーザまたはグループに再割り当てして、新しいノードをユーザまたはグループに追加する必要があります。

RBACユーザ / グループをクラスタ / DAGに再割り当てして、新しいノードをRBACユーザ / グループに追加する必要があります。たとえば、2ノード クラスタにRBACユーザまたはグループを割り当てたとします。このクラスタに別のノードを追加した場合は、RBACユーザ / グループをクラスタに再割り当てして、新しいノードをRBACユーザ / グループに追加する必要があります。

- Snapshotをレプリケートする場合は、処理を実行するユーザにソースとデスティネーションの両方のボリュームに対するストレージ接続を割り当てる必要があります。

ユーザにアクセスを割り当てる前にアセットを追加しておいてください。



SnapCenter Plug-in for VMware vSphereの機能を使用してVM、VMDK、またはデータストアを保護している場合は、VMware vSphere GUIを使用してSnapCenter Plug-in for VMware vSphereロールにvCenterユーザを追加する必要があります。VMware vSphere のロールの詳細については、以下を参照してください。 ["SnapCenter Plug-in for VMware vSphereに組み込みの事前定義のロール"](#)。

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. 設定ページで、ユーザーとアクセス > *をクリックします。  *。
3. [Active Directory またはワークグループからユーザ / グループを追加] ページで次の操作を実行します。

フィールド	操作
アクセスタイプ	[Domain]または[workgroup]を選択します。 ドメイン認証タイプの場合は、ロールに追加するユーザまたはグループのドメイン名を指定する必要があります。 デフォルトでは、ログインしているドメイン名があらかじめ入力されています。  信頼されていないドメインは、設定 > グローバル設定 > ドメイン設定 ページで登録する必要があります。
タイプ	[User]または[Group]を選択します。  SnapCenterでサポートされるのはセキュリティ グループのみです。配信グループはサポートされません。
ユーザ名	a. ユーザー名の一部を入力し、[追加] をクリックします。  ユーザ名では大文字と小文字が区別されます。 b. 検索リストからユーザ名を選択します。  別のドメインまたは信頼されないドメインからユーザを追加する場合、ドメインをまたぐユーザの検索リストはないため、完全なユーザ名を入力する必要があります。 同じ手順を繰り返して、選択したロールに必要なユーザまたはグループを追加します。
ロール	ユーザを追加するロールを選択します。

4. *割り当て*をクリックし、資産の割り当てページで次の操作を行います。
 - a. *資産*ドロップダウンリストから資産の種類を選択します。

b. 資産テーブルで、資産を選択します。

リストには、ユーザがSnapCenterに追加したアセットだけが表示されます。

c. 必要なすべてのアセットについて、同じ手順を繰り返します。

d. *保存*をクリックします。

5. *送信*をクリックします。

ユーザまたはグループを追加してロールを割り当てたら、リソース リストを更新します。

監査ログの設定

監査ログは、SnapCenter Serverのすべてのアクティビティについて生成されます。デフォルトでは、監査ログはデフォルトのインストール場所 `C:\Program Files\NetApp\SnapCenter WebApp\audit\` に保存されます。

監査ログのセキュリティは、すべての監査イベントについて、不正な変更ができないようにデジタル署名が付いたダイジェストを生成することで確保されます。生成されたダイジェストは、独立した監査チェックサムファイルに保持され、コンテンツの整合性を確認するために定期的な整合性チェックが実行されます。

「SnapCenterAdmin」ロールでログインする必要があります。

タスク概要

- アラートは、次のシナリオで送信されます。
 - 監査ログの整合性チェックのスケジュールまたはsyslogサーバが有効化 / 無効化された
 - 監査ログの整合性チェック、監査ログ、またはsyslogサーバ ログに問題がある
 - ディスク スペースが不足している
- 整合性チェックに失敗した場合のみ、Eメールが送信されます。
- 監査ログのディレクトリと監査チェックサム ログのディレクトリのパスは、両方とも変更する必要があります。片方だけを変更することはできません。
- 監査ログのディレクトリと監査チェックサム ログのディレクトリのパスを変更すると、以前の場所にある監査ログに対して整合性チェックを実行できなくなります。
- 監査ログのディレクトリと監査チェックサム ログのディレクトリのパスは、SnapCenter Serverのローカルドライブ上である必要があります。

共有ドライブやネットワーク マウント ドライブは、サポートされていません。

- syslogサーバの設定でUDPプロトコルを使用している場合、ポートが停止している、または使用できないことによるエラーは、SnapCenterでエラーまたはアラートとして取得できません。
- 監査ログを構成するには、Set-SmAuditSettings コマンドと Get-SmAuditSettings コマンドを使用できません。

コマンドレットで利用できるパラメータとその説明は、Get-Help command_nameを実行して確認できます。あるいは、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

手順

1. 設定*ページで、*設定 > グローバル設定 > *監査ログ設定*に移動します。
2. [Audit log]セクションで、詳細を入力します。
3. *監査ログディレクトリ*と*監査チェックサムログディレクトリ*を入力します。
 - a. [Maximum file size]を入力します。
 - b. [Maximum log files]を入力します。
 - c. アラートが送信されるディスク スペース使用量を割合（%）で入力します。
4. (オプション) **UTC** 時間のログ を有効にします。
5. (オプション) 監査ログ整合性チェックスケジュール を有効にし、オンデマンド整合性チェックを実行するために 整合性チェックの開始 をクリックします。

Start-SmAuditIntegrityCheck コマンドを実行して、オンデマンドの整合性チェックを開始することもできます。

6. (オプション) [Forwarded audit logs to remote syslog server]を有効にし、syslogサーバの詳細を入力します。

TLS 1.2プロトコルについては、syslogサーバから「信頼されたルート」に証明書をインポートする必要があります。

- a. syslogサーバのホストを入力します。
 - b. syslogサーバのポートを入力します。
 - c. syslogサーバのプロトコルを入力します。
 - d. RFCの形式を入力します。
7. *保存*をクリックします。
 8. モニター > ジョブ をクリックすると、監査整合性チェックとディスク容量チェックを確認できます。

SnapCenter ServerとのセキュアなMySQL接続の設定

スタンドアロン構成またはNetwork Load Balancing (NLB) 構成でSnapCenter ServerとMySQLサーバの間の通信を保護する場合は、Secure Sockets Layer (SSL) 証明書とキー ファイルを生成します。

スタンドアロンSnapCenter Server構成用のセキュアなMySQL接続の設定

SnapCenter ServerとMySQLサーバの間の通信を保護するには、Secure Sockets Layer (SSL) 証明書とキー ファイルを生成します。証明書とキー ファイルは、MySQLサーバとSnapCenter Serverで設定する必要があります。

次の証明書が生成されます。

- CA証明書
- サーバのパブリック証明書と秘密鍵ファイル
- クライアントのパブリック証明書と秘密鍵ファイル

手順

1. opensslコマンドを使用して、WindowsのMySQLサーバおよびクライアントのSSL証明書とキー ファイルを設定します。

詳細については、"[MySQL バージョン 5.7: openssl を使用した SSL 証明書とキーの作成](#)"



サーバ証明書、クライアント証明書、およびキー ファイルに使用する共通名は、それぞれCA証明書の共通名と異なる必要があります。共通名が同じ場合、それらの証明書とキー ファイルはOpenSSLを使用してコンパイルされたサーバでエラーになります。

ベスト プラクティス: サーバー証明書の共通名として、サーバーの完全修飾ドメイン名 (FQDN) を使用する必要があります。

2. SSL証明書とキー ファイルをMySQLのデータ フォルダにコピーします。

デフォルトのMySQLデータフォルダのパスは C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\。

3. MySQLサーバ構成ファイル (my.ini) で、CA証明書、サーバ パブリック証明書、クライアント パブリック証明書、サーバ秘密鍵、およびクライアント秘密鍵のパスを更新します。

デフォルトのMySQLサーバ設定ファイル (my.ini) のパスは
C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini。



MySQL サーバ構成ファイル (my.ini) の [mysqld] セクションで、CA 証明書、サーバ公開証明書、およびサーバ秘密キーのパスを指定する必要があります。

MySQL サーバ構成ファイル (my.ini) の [client] セクションで、CA 証明書、クライアント公開証明書、およびクライアント秘密キーのパスを指定する必要があります。

次の例は、デフォルトフォルダのmy.iniファイルの[mysqld]セクションにコピーされた証明書とキーファイルを示しています。 C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data 。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

次の例は、my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
key.pem"
```

4. Internet Information Server (IIS) でSnapCenter Server Webアプリケーションを停止します。
5. MySQLサービスを再起動します。
6. SnapManager.Web.UI.dll.configファイルのMySQLProtocolキーの値を更新します。

次の例では、SnapManager.Web.UI.dll.configファイルのMySQLProtocolキーの値が更新されています。

```
<add key="MySQLProtocol" value="SSL" />
```

7. my.ini ファイルの [client] セクションで指定されたパスを使用して、SnapManager.Web.UI.dll.config ファイルを更新します。

次の例は、my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/ca.pem" />
```

8. IISでSnapCenter Server Webアプリケーションを起動します。

HA構成用のセキュアなMySQL接続の設定

SnapCenter ServerとMySQLサーバの間の通信を保護する場合は、両方の高可用性（HA）ノード用にSecure Sockets Layer（SSL）証明書とキー ファイルを生成します。証明書とキー ファイルは、MySQLサーバとHAノードで設定する必要があります。

次の証明書が生成されます。

- CA証明書

一方のHAノードでCA証明書を生成し、もう一方のHAノードにコピーします。

- 両方のHAノードのサーバパブリック証明書とサーバ秘密鍵ファイル
- 両方のHAノードのクライアントパブリック証明書とクライアント秘密鍵ファイル

手順

1. 1つ目のHAノードで、opensslコマンドを使用して、WindowsのMySQLサーバおよびクライアントのSSL証明書とキー ファイルを設定します。

詳細については、"[MySQL バージョン 5.7: openssl を使用した SSL 証明書とキーの作成](#)"



サーバ証明書、クライアント証明書、およびキー ファイルに使用する共通名は、それぞれCA証明書の共通名と異なる必要があります。共通名が同じ場合、それらの証明書とキー ファイルはOpenSSLを使用してコンパイルされたサーバでエラーになります。

ベスト プラクティス: サーバー証明書の共通名として、サーバーの完全修飾ドメイン名 (FQDN) を使用する必要があります。

2. SSL証明書とキー ファイルをMySQLのデータ フォルダにコピーします。

MySQLのデータ フォルダのデフォルト パスは、C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\ です。

3. MySQLサーバ構成ファイル (my.ini) で、CA証明書、サーバパブリック証明書、クライアントパブリック証明書、サーバ秘密鍵、およびクライアント秘密鍵のパスを更新します。

MySQLサーバ構成ファイル (my.in) のデフォルト パスは、C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.iniです



MySQL サーバー構成ファイル (my.ini) の [mysqld] セクションで、CA 証明書、サーバー公開証明書、およびサーバー秘密キーのパスを指定する必要があります。

MySQL サーバー構成ファイル (my.ini) の [client] セクションで、CA 証明書、クライアント公開証明書、およびクライアント秘密キーのパスを指定する必要があります。

次の例は、デフォルト フォルダ C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data にある my.ini ファイルの [mysqld] セクションにコピーされた証明書とキー ファイルを示しています。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

次の例は、my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
key.pem"
```

4. 2つ目のHAノードで、次の手順に従ってCA証明書をコピーし、サーバパブリック証明書、サーバ秘密鍵ファイル、クライアントパブリック証明書、およびクライアント秘密鍵ファイルを生成します。

- a. 1つ目のHAノードで生成したCA証明書を2つ目のHAノードのMySQLのデータフォルダにコピーします。

MySQLのデータフォルダのデフォルトパスは、C:\ProgramData\NetApp\SnapCenter\MySQL Data\Dataです。



CA証明書は新しく作成しないでください。サーバパブリック証明書、クライアントパブリック証明書、サーバ秘密鍵ファイル、クライアント秘密鍵ファイルのみを作成します。

- b. 1つ目のHAノードで、opensslコマンドを使用して、WindowsのMySQLサーバおよびクライアントのSSL証明書とキーファイルを設定します。

"MySQL バージョン 5.7: openssl を使用した SSL 証明書とキーの作成"



サーバ証明書、クライアント証明書、およびキーファイルに使用する共通名は、それぞれCA証明書の共通名と異なる必要があります。共通名が同じ場合、それらの証明書とキーファイルはOpenSSLを使用してコンパイルされたサーバでエラーになります。

サーバ証明書の共通名としてサーバのFQDNを使用することを推奨します。

- c. SSL証明書とキーファイルをMySQLのデータフォルダにコピーします。
- d. MySQLサーバ構成ファイル (my.ini) で、CA証明書、サーバパブリック証明書、クライアントパブリック証明書、サーバ秘密鍵、およびクライアント秘密鍵のパスを更新します。



MySQL サーバ構成ファイル (my.ini) の [mysqld] セクションで、CA 証明書、サーバ公開証明書、およびサーバ秘密キーのパスを指定する必要があります。

MySQL サーバー構成ファイル (my.ini) の [client] セクションで、CA 証明書、クライアント公開証明書、およびクライアント秘密キーのパスを指定する必要があります。

次の例は、デフォルト フォルダ C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data にある my.ini ファイルの [mysqld] セクションにコピーされた証明書とキー ファイルを示しています。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

次の例は、my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

5. 両方のHAノードのInternet Information Server (IIS) でSnapCenter Server Webアプリケーションを停止します。
6. 両方のHAノードで、MySQLサービスを再起動します。
7. 両方のHAノードで、SnapManager.Web.UI.dll.configファイルのMySQLProtocolキーの値を更新します。

次の例では、SnapManager.Web.UI.dll.configファイルのMySQLProtocolキーの値が更新されています。

```
<add key="MySQLProtocol" value="SSL" />
```

8. 両方の HA ノードの my.ini ファイルの [client] セクションで指定したパスを使用して、SnapManager.Web.UI.dll.config ファイルを更新します。

次の例は、my.ini ファイルの [client] セクションで更新されたパスを示しています。

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/ca.pem" />
```

9. 両方のHAノードのIISでSnapCenter Server Webアプリケーションを起動します。
10. 一方のHAノードで、PowerShellのSet-SmRepositoryConfig -RebuildSlave -Forceコマンドレット（-Forceオプションを指定）を使用して、両方のHAノードにセキュアなMySQLレプリケーションを確立します。

レプリケーションが健全な状態であっても、-Forceオプションを指定するとスレーブ リポジトリを再構築できます。

証明書ベースの認証を構成する

証明書ベースの認証は、SnapCenterサーバーとプラグイン ホストの両方の ID を検証することでセキュリティを強化し、安全で暗号化された通信を保証します。

証明書ベースの認証の有効化

SnapCenter ServerおよびWindowsプラグイン ホストの証明書ベースの認証を有効にするには、次のPowerShellコマンドレットを実行します。Linuxプラグイン ホストで双方向SSLを有効にすると、証明書ベースの認証が有効になります。

- クライアント証明書ベースの認証を有効にする：

```
Set-SmConfigSettings -Agent -configSettings  
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- クライアント証明書ベースの認証を無効にする：

```
Set-SmConfigSettings -Agent -configSettings  
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]
```

SnapCenter Serverからの認証局（CA）証明書のエクスポート

Microsoft管理コンソール（MMC）を使用して、SnapCenter Serverからプラグイン ホストにCA証明書をエクスポートする必要があります。

開始する前に

双方向SSLを設定しておく必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、コンピューター アカウント オプションを選択し、完了 をクリックします。
4. コンソール ルート > 証明書 - ローカル コンピューター > 個人 > 証明書 をクリックします。
5. SnapCenter Server に使用される取得した CA 証明書を右クリックし、[すべてのタスク] > [エクスポート] を選択してエクスポート ウィザードを起動します。
6. ウィザードで次の操作を実行します。

オプション	操作
秘密キーのエクスポート	*いいえ、秘密キーをエクスポートしません*を選択し、*次へ*をクリックします。
エクスポート ファイルの形式	*次へ*をクリックします。
ファイル名	*参照*をクリックし、証明書を保存するファイル パスを指定して、*次へ*をクリックします。
証明書のエクスポート ウィザードの完了	概要を確認し、[完了] をクリックしてエクスポートを開始します。



証明書ベースの認証は、SnapCenter HA構成およびSnapCenter Plug-in for VMware vSphereではサポートされません。

Windows プラグインホストにCA証明書をインポートする

エクスポートしたSnapCenter Server CA証明書を使用するには、Microsoft管理コンソール（MMC）を使用して、関連する証明書をSnapCenter Windowsプラグイン ホストにインポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、コンピューター アカウント オプションを選択し、完了 をクリックします。
4. コンソール ルート > 証明書 - ローカル コンピューター > 個人 > 証明書 をクリックします。
5. 「個人」フォルダを右クリックし、[すべてのタスク] > [インポート] を選択して、インポート ウィザード

を起動します。

6. ウィザードで次の操作を実行します。

オプション	操作
保存場所	*次へ*をクリックします。
インポートするファイル	拡張子.cerで終わるSnapCenter Server証明書を選択します。
証明書ストア	*次へ*をクリックします。
証明書のエクスポート ウィザードの完了	概要を確認し、[完了] をクリックしてインポートを開始します。

UNIXプラグイン ホストへのCA証明書のインポート

CA証明書をUNIXプラグイン ホストにインポートする必要があります。

このタスクについて

- SPLキーストアのパスワード、および使用中のCA署名キー ペアのエイリアスを管理できます。
- SPLキーストアのパスワードと、秘密キーに関連付けられているエイリアス パスワードをすべて同じにする必要があります。

手順

1. SPLキーストアのデフォルト パスワードは、SPLプロパティ ファイルから取得できます。キーに対応する値です `SPL_KEYSTORE_PASS`。
2. キーストアのパスワードを変更します。
`$ keytool -storepasswd -keystore keystore.jks`
3. キーストア内の秘密鍵エントリのすべてのエイリアスのパスワードを、キーストアで使用されているものと同じパスワードに変更します。
`$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. キー`SPL_KEYSTORE_PASS`も同様に更新します。`spl.properties`ファイル。
5. パスワードを変更したら、サービスを再起動します。

ルート証明書または中間証明書の**SPL**トラストストアへの設定

ルート証明書または中間証明書をSPLトラストストアに設定する必要があります。ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

手順

1. SPL キーストアが含まれているフォルダーに移動します。 `/var/opt/snapcenter/spl/etc`。
2. ファイルを見つける `keystore.jks`。

3. キーストアに追加された証明書を一覧表示します。
\$ keytool -list -v -keystore keystore.jks
4. ルート証明書または中間証明書を追加します。
\$ keytool -import -trustcacerts -alias <AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore keystore.jks
5. SPLトラストストアへのルート証明書または中間証明書を設定したら、サービスを再起動します。

SPLトラストストアに対するCA署名付きキー ペアの設定

SPLトラストストアに対してCA署名付きキー ペアを設定する必要があります。

手順

1. SPLのキーストアを含むフォルダに移動します /var/opt/snapcenter/spl/etc。
2. ファイルを見つける keystore.jks`。
3. キーストアに追加された証明書を一覧表示します。
\$ keytool -list -v -keystore keystore.jks
4. 秘密鍵と公開鍵の両方を持つ CA 証明書を追加します。
\$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
5. キーストアに追加された証明書を一覧表示します。
\$ keytool -list -v -keystore keystore.jks
6. キーストアに追加された新しいCA証明書に対応するエイリアスが、キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのSPLキーストアのパスワードは、SPL_KEYSTORE_PASSキーの値です。`spl.properties`ファイル。

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
```

8. CA 証明書のエイリアス名が長く、スペースや特殊文字 (「*」、「」) が含まれている場合は、エイリアス名を単純な名前に変更します。
\$ keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. 以下のキーストアからエイリアス名を設定します。`spl.properties`ファイル。SPL_CERTIFICATE_ALIAS キーに対するこの値を更新します。
10. SPLトラストストアにCA署名キー ペアを設定したら、サービスを再起動します。

SnapCenter証明書のエクスポート

SnapCenter証明書を .pfx 形式でエクスポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、[ユーザー アカウント] オプションを選択し、[完了] をクリックします。
4. コンソール ルート > 証明書 - 現在のユーザー > 信頼されたルート証明機関 > 証明書 をクリックします。
5. SnapCenterフレンドリ名を持つ証明書を右クリックし、[すべてのタスク] > [エクスポート] を選択してエクスポート ウィザードを開始します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのエクスポート	*はい、秘密キーをエクスポートします*オプションを選択し、*次へ*をクリックします。
エクスポート ファイルの形式	変更せずに、[次へ] をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、[次へ] をクリックします。
エクスポートするファイル	エクスポートする証明書のファイル名を指定し (.pfx を使用する必要があります)、[次へ] をクリックします。
証明書のエクスポート ウィザードの完了	概要を確認し、[完了] をクリックしてエクスポートを開始します。

WindowsホストのCA証明書の設定

CA証明書CSRファイルの生成

証明書署名要求 (CSR) を生成し、生成したCSRを使用して認証局 (CA) から取得した証明書をインポートできます。証明書には秘密キーが関連付けられます。

CSRはエンコードされたテキストのブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。



CA 証明書の RSA キーの長さは最低 3072 ビットである必要があります。

CSRを生成するための情報については、["CA証明書CSRファイルの生成方法"](#)。



ドメイン (*.domain.company.com) またはシステム (machine1.domain.company.com) の CA 証明書を所有している場合は、CA 証明書 CSR ファイルの生成をスキップできます。SnapCenterを使用して、既存のCA証明書を導入できます。

クラスタ構成の場合、クラスタ名（仮想クラスタFQDN）と、それぞれのホスト名がCA証明書に記載されている必要があります。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。ワイルドカード証明書 (*.domain.company.com) の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenter ServerとWindowsホスト プラグインにCA証明書をインポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル]>[スナップインの追加と削除] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
4. コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書 をクリックします。
5. 「信頼されたルート証明機関」フォルダを右クリックし、[すべてのタスク]>[インポート] を選択して、インポート ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*次へ*をクリックします。
インポート ファイル形式	変更せずに、[次へ] をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、[次へ] をクリックします。
証明書のインポート ウィザードの完了	概要を確認し、[完了] をクリックしてインポートを開始します。



インポートする証明書は秘密キーとバンドルされている必要があります (サポートされている形式は **.pfx**、**.p12**、および ***.p7b** です)。

7. 「個人用」フォルダに対して手順5を繰り返します。

CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための16進数の文字列です。サムプリントは、サムプリント アルゴリズムを使用して証明書の内容から計算されます。

手順

1. GUIで次の手順を実行します。
 - a. 証明書をダブルクリックします。
 - b. [証明書] ダイアログボックスで、[詳細] タブをクリックします。
 - c. フィールドのリストをスクロールして、「拇印」をクリックします。
 - d. ボックスから16進数の文字をコピーします。
 - e. 16進数の間のスペースを削除します。

たとえば、拇印が「a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b」の場合、スペースを削除すると「a909502dd82ae41433e6f83886b00d4277a32a7b」になります。

2. PowerShellで、次の手順を実行します。
 - a. 次のコマンドを実行して、インストールされている証明書のサムプリントを表示し、最近インストールされた証明書をサブジェクト名で識別します。

```
Get-ChildItem -Path 証明書:\LocalMachine\My
```

- b. サムプリントをコピーします。

Windowsホスト プラグイン サービスでのCA証明書の設定

インストールされているデジタル証明書をアクティブ化するには、Windowsホスト プラグイン サービスを使用してCA証明書を設定する必要があります。

SnapCenter Serverと、CA証明書がすでに導入されているすべてのプラグイン ホストで、次の手順を実行します。

手順

1. 次のコマンドを実行して、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例えば：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

． 次のコマンドを実行して、新しくインストールした証明書をWindowsホスト プラグイン サービスとバインドします。

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例えば：


```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

SnapCenterサイトでのCA証明書の設定

Windowsホスト上のSnapCenterサイトでCA証明書を設定する必要があります。

手順

1. SnapCenterがインストールされているWindows Serverで、IISマネージャを開きます。
2. 左側のナビゲーション ペインで、[接続] をクリックします。
3. サーバーの名前と*サイト*を展開します。
4. SSL証明書をインストールするSnapCenterのWebサイトを選択します。
5. アクション > サイトの編集 に移動し、バインド をクリックします。
6. [バインディング] ページで、*https のバインディング*を選択します。
7. *編集*をクリックします。
8. [SSL certificate] ドロップダウン リストから、最近インポートしたSSL証明書を選択します。
9. [OK]をクリックします。



SnapCenter Scheduler サイト (デフォルト ポート: 8154、HTTPS) は、自己署名証明書で構成されています。このポートはSnapCenter Serverホスト内で通信しており、CA証明書を使用した設定は必須ではありません。ただし、CA証明書の使用が必要な環境の場合は、SnapCenterスケジューラ サイトを使用して手順5から9を繰り返します。



最近導入したCA証明書がドロップダウン メニューに表示されない場合は、CA証明書が秘密鍵に関連付けられているかどうかを確認します。



次のパスを使用して証明書が追加されていることを確認します: コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書。

SnapCenterのCA証明書の有効化

CA証明書を設定し、SnapCenter ServerのCA証明書の検証を有効にする必要があります。

開始する前に

- CA証明書を有効または無効にするには、Set-SmCertificateSettingsコマンドレットを使用します。
- SnapCenter Serverの証明書のステータスを表示するには、Get-SmCertificateSettingsコマンドレットを使用します。

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。または、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. 設定ページで、設定 > グローバル設定 > **CA 証明書設定** に移動します。
2. *証明書の検証を有効にする*を選択します。
3. *適用*をクリックします。

終わったら

[Managed Hosts]タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Serverとプラグイン ホスト間の接続のステータスを示します。

- *🔑* は、プラグイン ホストに有効化されているか割り当てられている CA 証明書がないことを示します。
- *🟢* は CA 証明書が正常に検証されたことを示します。
- *🔴* は、CA 証明書を検証できなかったことを示します。
- *🔴?* は接続情報を取得できなかったことを示します。



ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

LinuxホストのCA証明書の設定

LinuxにSnapCenter Serverをインストールすると、インストーラによって自己署名証明書が作成されます。このCA証明書を使用する場合は、nginxリバース プロキシ、監査ログ、およびSnapCenterサービスの証明書を設定する必要があります。

nginx証明書の設定

手順

1. `/etc/nginx/conf.d` に移動します。 `cd /etc/nginx/conf.d`
2. vi または任意のテキスト エディターを使用して **snapcenter.conf** を開きます。
3. 構成ファイルのserverセクションに移動します。
4. CA 証明書を指すように `ssl_certificate` と `ssl_certificate_key` のパスを変更します。
5. ファイルを保存して、閉じます。
6. nginx をリロードします: `$nginx -s reload`

監査ログ証明書の設定

手順

1. vi または任意のテキスト エディターを使用して、`INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config` を開きます。

`INSTALL_DIR` のデフォルト値は `/opt` です。

2. **AUDILOG_CERTIFICATE_PATH** キーと **AUDILOG_CERTIFICATE_PASSWORD** キーを編集して、それぞれ CA 証明書パスとパスワードを含めます。

監査ログ証明書では `.pfx` 形式のみがサポートされます。

3. ファイルを保存して、閉じます。
4. **snapmanagerweb** サービスを再起動します。 `$ systemctl restart snapmanagerweb`

SnapCenterサービス証明書の設定

手順

1. viまたは任意のテキスト エディタを使用して、次の構成ファイルを開きます。
 - `INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config`
 - `INSTALL_DIR/NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config`
 - `INSTALL_DIR/NetApp/snapcenter/Scheduler/Scheduler.Api.dll.config`

`INSTALL_DIR` のデフォルト値は `/opt` です。

2. **SERVICE_CERTIFICATE_PATH** キーと **SERVICE_CERTIFICATE_PASSWORD** キーを編集して、それぞれ CA 証明書パスとパスワードを含めます。

SnapCenterサービス証明書では、`.pfx` 形式のみがサポートされます。

3. ファイルを保存して閉じます。
4. すべてのサービスを再起動します。
 - `$ systemctl restart snapmanagerweb`
 - `$ systemctl restart smcore`
 - `$ systemctl restart scheduler`

Windowsホストでの双方向SSL通信の設定と有効化

Windowsホストでの双方向SSL通信の設定

Windowsホスト上のSnapCenter Serverとプラグインの間の相互通信を保護するために、双方向SSL通信を設定する必要があります。

開始する前に

- サポートされるキーの最小長が3072のCA証明書CSRファイルを生成しておく必要があります。
- CA証明書でサーバ認証とクライアント認証がサポートされている必要があります。
- 秘密キーとサムプリントの詳細が記載されたCA証明書が必要です。
- 一方向SSL設定を有効にしておく必要があります。

詳細については、"[CA 証明書セクション](#)を構成します。"

- すべてのプラグイン ホストとSnapCenter Serverで双方向SSL通信を有効にしておく必要があります。

双方向SSL通信が一部のホストまたはサーバで有効になっていない環境はサポートされていません。

手順

1. ポートをバインドするには、SnapCenter Serverホストで次の手順を実行します。この手順はPowerShell コマンドを使用してSnapCenter IIS Webサーバのポート8146（デフォルト）で行ったあと、SMCoreポート8145（デフォルト）でも行います。

- a. 次のPowerShellコマンドを使用して、既存のSnapCenter自己署名証明書のポート バインドを削除します。

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
```

次に例を示します。

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

```
> netsh http delete sslcert ipport=0.0.0.0:8146
```

- b. 新しく取得したCA証明書をSnapCenter ServerとSMCoreポートにバインドします。

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>  
certhash=$cert appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

次に例を示します。

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8146
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

2. CA 証明書へのアクセス許可を得るには、次の手順を実行して、新しく取得した CA 証明書にアクセスし、証明書のアクセス許可リストに SnapCenter のデフォルトの IIS Web サーバー ユーザー「**IIS AppPool\ SnapCenter**」を追加します。
 - a. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。
 - b. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
 - c. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
 - d. コンソール ルート > 証明書 - ローカル コンピューター > 個人 > 証明書 をクリックします。
 - e. SnapCenter証明書を選択します。
 - f. ユーザー\権限の追加ウィザードを開始するには、CA 証明書を右クリックし、[すべてのタスク] > [秘密キーの管理] を選択します。
 - g. *追加*をクリックし、ユーザーとグループの選択ウィザードで場所をローカルコンピューター名（階層の最上位）に変更します。
 - h. IIS AppPool\SnapCenterユーザを追加し、フル コントロール権限を付与します。
3. **CA 証明書 IIS** アクセス許可 については、次のパスから SnapCenter Server に新しい DWORD レジストリ キー エントリを追加します。

Windowsレジストリ エディタで次のパスに移動します。

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
```

4. SCHANNELレジストリ設定のコンテキストで、新しいDWORDレジストリ キー エントリを作成します。

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```

双方向SSL通信のSnapCenter Windows プラグインの設定

PowerShellコマンドを使用して、SnapCenter Windowsプラグインで双方向SSL通信を使用できるように設定する必要があります。

開始する前に

CA証明書サムプリントが使用可能であることを確認します。

手順

1. ポートをバインドするには、Windowsプラグイン ホストでSMCoreポート8145（デフォルト）に対して次の操作を実行します。
 - a. 次のPowerShellコマンドを使用して、既存のSnapCenter自己署名証明書のポート バインドを削除します。

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
```

次に例を示します。

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- b. 新しく取得したCA証明書をSMCoreポートにバインドします。

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert  
appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
```

次に例を示します。

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

Windowsホストでの双方向SSL通信の有効化

PowerShellコマンドを使用して、双方向SSL通信を有効にし、Windowsホスト上のSnapCenter Serverとプラグインの間の相互通信を保護できます。

始める前に

すべてのプラグインとSMCoreエージェントのコマンドを実行したあと、サーバのコマンドを実行します。

手順

1. 双方向SSL通信を有効にするには、SnapCenter Serverで、プラグイン、サーバ、および双方向SSL通信が必要な各エージェントに対して次のコマンドを実行します。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName <Plugin_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. 次のコマンドを使用して、IIS SnapCenterアプリケーション プールのリサイクル操作を実行します。

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. Windowsプラグインの場合は、次のPowerShellコマンドを実行してSMCoreサービスを再起動します。

```
> Restart-Service -Name SnapManagerCoreService
```

双方向SSL通信の無効化

PowerShellコマンドを使用して、双方向SSL通信を無効にすることができます。

このタスクについて

- すべてのプラグインとSMCoreエージェントのコマンドを実行したあと、サーバのコマンドを実行します。
- 双方向SSL通信を無効にしても、CA証明書とその設定は削除されません。
- SnapCenter Serverに新しいホストを追加するには、すべてのプラグイン ホストで双方向SSLを無効にする必要があります。
- NLBとF5はサポートされません。

手順

1. 双方向SSL通信を無効にするには、SnapCenter Serverですべてのプラグイン ホストとSnapCenterホストに対して次のコマンドを実行します。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName <Agent_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. 次のコマンドを使用して、IIS SnapCenterアプリケーション プールのリサイクル操作を実行します。

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. Windowsプラグインの場合は、次のPowerShellコマンドを実行してSMCoreサービスを再起動します。

```
> Restart-Service -Name SnapManagerCoreService
```

Linuxホストでの双方向SSL通信の設定と有効化

Linuxホストでの双方向SSL通信の設定

Linuxホスト上のSnapCenter Serverとプラグインの間の相互通信を保護するために、双方向SSL通信を設定する必要があります。

開始する前に

- LinuxホストのCA証明書を設定しておく必要があります。
- すべてのプラグイン ホストとSnapCenter Serverで双方向SSL通信を有効にしておく必要があります。

手順

1. **certificate.pem** を `/etc/pki/ca-trust/source/anchors/` にコピーします。

2. Linuxホストの信頼リストに証明書を追加します。

- `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
- `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
- `update-ca-trust extract`

3. 証明書が信頼リストに追加されたかどうかを確認します。

`trust list | grep "<CN of your certificate>"`

4. SnapCenter **nginx** ファイル内の **ssl_certificate** と **ssl_certificate_key** を更新して再起動します。

- `vim /etc/nginx/conf.d/snapcenter.conf`
- `systemctl restart nginx`

5. SnapCenter Server GUIリンクを更新します。

6. /<インストール パス>/ *NetApp/snapcenter/SnapManagerWeb* にある * *SnapManager.Web.UI.dll.config** と /<インストール パス>/ *NetApp/snapcenter/SMCore* にある **SMCoreServiceHost.dll.config** の次のキーの値を更新します。

- `<add key="SERVICE_CERTIFICATE_PATH" value="<certificate.pfx のパス>" />`
- `<キーを追加="SERVICE_CERTIFICATE_PASSWORD" 値="<パスワード>" />`

7. 次のサービスを再起動します。

- `systemctl restart smcore.service`
- `systemctl restart snapmanagerweb.service`

8. 証明書がSnapManager Web ポートに接続されていることを確認します。

`openssl s_client -connect localhost:8146 -brief`

9. 証明書が smcore ポートに接続されていることを確認します。

`openssl s_client -connect localhost:8145 -brief`

10. SPLキーストアとエイリアスのパスワードを管理します。

- SPL プロパティ ファイルの **SPL_KEYSTORE_PASS** キーに割り当てられた SPL キーストアのデフォルト パスワードを取得します。
- キーストアのパスワードを変更します。
`keytool -storepasswd -keystore keystore.jks`
- すべての秘密鍵エントリのエイリアスのパスワードを変更します。
`keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
- spl.properties* のキー **SPL_KEYSTORE_PASS** の同じパスワードを更新します。
- サービスを再起動します。

11. プラグインのLinuxホストで、SPLプラグインのキーストアにルート証明書と中間証明書を追加します。

- `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties file>`
- `keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS`

- i. keystore.jks 内のエントリを確認します。

```
keytool -list -v -keystore <path to keystore.jks>
```

- ii. 必要に応じてエイリアスの名前を変更します。

```
keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass  
keypass -keystore </path/to/keystore> -storepass storepas
```

12. `spl.properties` ファイルの **SPL_CERTIFICATE_ALIAS** の値を、`keystore.jks` に保存されている **certificate.pfx** のエイリアスで更新し、SPL サービスを再起動します。 `systemctl restart spl`

13. 証明書が `smcore` ポートに接続されていることを確認します。

```
openssl s_client -connect localhost:8145 -brief
```

LinuxホストでのSSL通信の有効化

PowerShellコマンドを使用して、双方向SSL通信を有効にし、Linuxホスト上のSnapCenter Serverとプラグインの間の相互通信を保護できます。

手順

1. 次の手順を実行して、一方向SSL通信を有効にします。
 - a. SnapCenter GUIにログインします。
 - b. 設定 > グローバル設定 をクリックし、* SnapCenterサーバーで証明書の検証を有効にする* を選択します。
 - c. ホスト > 管理対象ホスト をクリックし、一方向 SSL を有効にするプラグイン ホストを選択します。
 - d. クリック  アイコンをクリックし、[証明書の検証を有効にする] をクリックします。
2. SnapCenter ServerのLinuxホストから双方向SSL通信を有効にします。
 - `Open-SmConnection`
 - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName <Plugin Host Name>`
 - `Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"} -HostName localhost`
 - `Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}`

Active Directory、LDAP、LDAPSの設定

信頼されていないActive Directoryドメインの登録

信頼されていない複数のActive Directoryドメインのホスト、ユーザ、およびグループを管理するには、Active DirectoryをSnapCenter Serverに登録する必要があります。

開始する前に

LDAP および LDAPS プロトコル

- 信頼されていないActive Directoryドメインは、LDAPプロトコルまたはLDAPSプロトコルを使用して登録できます。

- プラグイン ホストとSnapCenter Serverの間の双方向の通信を有効にしておく必要があります。
- SnapCenter Serverとプラグイン ホストの間でDNS解決が設定されている必要があります。

LDAPプロトコル

- 完全修飾ドメイン名（FQDN）をSnapCenter Serverから解決できる必要があります。

信頼されていないドメインはFQDNを使用して登録できます。FQDNをSnapCenter Serverから解決できない場合は、ドメイン コントローラのIPアドレスを使用して登録できます。このアドレスは、SnapCenter Serverから解決できるものである必要があります。

LDAPSプロトコル

- Active Directoryとの通信中にLDAPSでエンドツーエンドの暗号化を提供するためには、CA証明書が必要です。

"LDAPS用のCAクライアント証明書の設定"

- ドメイン コントローラのホスト名（DCHostName）にSnapCenter Serverから到達できる必要があります。

このタスクについて

- 信頼されていないドメインは、SnapCenterユーザ インターフェイス、PowerShellコマンドレット、REST APIのいずれかを使用して登録できます。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[グローバル設定]をクリックします。
3. [グローバル設定]ページで、[ドメイン設定]をクリックします。
4. をクリックし  で新しいドメインを登録します。
5. 「新しいドメインの登録」 ページで、**LDAP** または **LDAPS** のいずれかを選択します。
 - a. **LDAP** を選択した場合は、信頼されていないドメインを LDAP に登録するために必要な情報を指定します。

フィールド	操作
ドメイン名	ドメインのNetBIOS名を指定します。
ドメインFQDN	FQDN を指定して、[解決] をクリックします。

フィールド	操作
ドメインコントローラのIPアドレス	ドメインのFQDNをSnapCenter Serverから解決できない場合、ドメイン コントローラのIPアドレスを1つ以上指定します。 詳細については、以下を参照してください。 "GUIから信頼されていないドメインのドメインコントローラIPを追加する" 。

- b. **LDAPS** を選択した場合は、信頼されていないドメインを LDAPS に登録するために必要な情報を指定します。

フィールド	操作
ドメイン名	ドメインのNetBIOS名を指定します。
ドメインFQDN	FQDNを指定します。
Domain controller Names	1つ以上のドメイン コントローラ名を指定し、[解決] をクリックします。
ドメインコントローラのIPアドレス	ドメイン コントローラ名をSnapCenter Serverから解決できない場合は、DNS解決を修正する必要があります。

6. [OK]をクリックします。

Active Directoryの読み取り権限を有効にするためのIISアプリケーション プールの設定

SnapCenterの Active Directory 読み取り権限を有効にする必要がある場合は、Windows Server でインターネット インフォメーション サービス (IIS) を構成してカスタム アプリケーション プール アカウントを作成できます。

手順

1. SnapCenterがインストールされているWindows Serverで、IISマネージャを開きます。
2. 左側のナビゲーション ウィンドウで、[アプリケーション プール] をクリックします。
3. アプリケーション プール リストでSnapCenterを選択し、操作ウィンドウで 詳細設定 をクリックします。
4. [ID] を選択し、[...] をクリックしてSnapCenterアプリケーション プール ID を編集します。
5. [カスタム アカウント] フィールドに、Active Directory の読み取り権限を持つドメイン ユーザーまたはドメイン管理者のアカウント名を入力します。
6. [OK]をクリックします。

カスタム アカウントは、 SnapCenterアプリケーション プールの組み込み ApplicationPoolIdentity アカウ

ントを置き換えます。

LDAPS用のCAクライアント証明書の設定

Windows Active Directory LDAPSにCA証明書が設定されている場合は、SnapCenter ServerにLDAPSのCAクライアント証明書を設定する必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
4. コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書 をクリックします。
5. 「信頼されたルート証明機関」フォルダを右クリックし、[すべてのタスク] > [インポート] を選択して、インポート ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
ウィザードの2番目のページ	*参照*をクリックし、_ルート証明書_を選択して*次へ*をクリックします。
証明書のインポート ウィザードの完了	概要を確認し、[完了] をクリックしてインポートを開始します。

7. 中間証明書に対して手順 5 と 6 を繰り返します。

Microsoft SQL Serverデータベースの保護

SnapCenter Plug-in for Microsoft SQL Server

SnapCenter Plug-in for Microsoft SQL Serverの概要

SnapCenter Plug-in for Microsoft SQL Server は、Microsoft SQL Server データベースのアプリケーション対応のデータ保護管理を可能にするNetApp SnapCenterソフトウェアのホスト側コンポーネントです。Plug-in for SQL Serverを使用することで、SnapCenter環境でのSQL Serverデータベースのバックアップ、検証、リストア、クローニングの処理を自動化できます。

SQL Server 用プラグインがインストールされている場合は、SnapCenter をNetApp SnapMirrorテクノロジーと組み合わせて使用して、別のボリュームにバックアップセットのミラー コピーを作成したり、NetApp SnapVaultテクノロジーと組み合わせて使用して、標準コンプライアンスまたはアーカイブの目的でディスク間のバックアップ レプリケーションを実行したりできます。

- SnapCenter環境のMicrosoft SQL Serverデータベースに対するアプリケーション対応のバックアップ、リストア、クローニングの各処理が自動化されます。
- SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録した場合、VMDKおよびrawデバイス マッピング（RDM）LUN上のMicrosoft SQL Serverデータベースがサポートされます。
- SMB共有のプロビジョニングのみがサポートされます。SMB共有でのSQL Serverデータベースのバックアップはサポートされません。
- SnapManager for Microsoft SQL ServerからSnapCenterへのバックアップのインポートがサポートされます。

SnapCenter Plug-in for Microsoft SQL Serverの機能

SnapCenter Plug-in for Microsoft SQL Serverをインストールした環境では、SnapCenterを使用してSQL Serverデータベースをバックアップ、リストア、クローニングすることができます。

SQL Serverデータベースとデータベース リソースのバックアップ処理、リストア処理、クローニング処理をサポートする、次のタスクを実行できます。

- SQL Serverデータベースと関連するトランザクション ログをバックアップする

masterシステム データベースとmsdbシステム データベースについては、ログ バックアップを作成できません。modelシステム データベースのログ バックアップは作成できます。

- データベース リソースをリストアする
 - マスター システム データベース、msdbシステム データベース、モデル システム データベースをリストアできます。
 - 複数のデータベース、インスタンス、可用性グループのリストアはできません。
 - システム データベースは、別のパスにはリストアできません。

- 本番環境のデータベースのポイントインタイム クローンを作成する

tempdbシステム データベースに対して、バックアップ、リストア、クローニング、クローン ライフサイクルの各処理は実行できません。

- バックアップ処理をただちに検証するか、あとで検証する

SQL Serverシステム データベースの検証はサポートされていません。SnapCenterは、検証処理を実行するためにデータベースをクローニングします。SnapCenterは、SQL Serverシステム データベースをクローニングできません。そのため、これらのデータベースの検証はサポートされていません。

- バックアップ処理とクローニング処理のスケジュールを設定する
- バックアップ処理、リストア処理、クローニング処理を監視する



Plug-in for SQL Serverでは、SMB共有のSQL Serverデータベースのバックアップとリカバリはサポートされません。

SnapCenter Plug-in for Microsoft SQL Serverの特長

Plug-in for SQL Serverは、Windowsホスト上でMicrosoft SQL Serverデータベースと統合されるほか、システム上でNetApp Snapshotテクノロジーと統合されます。Plug-in for SQL Serverの操作には、SnapCenterのインターフェイスを使用します。

Plug-in for SQL Serverの主な機能は次のとおりです。

- * SnapCenterによる統合グラフィカル ユーザー インターフェイス*

SnapCenterのインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。どのプラグインでも、SnapCenterのインターフェイスから、バックアップ プロセスとリストア プロセスを一貫した方法で実行できるほか、ダッシュボード ビューで概要を把握したり、ロールベース アクセス制御 (RBAC) を設定したり、ジョブを監視したりすることができます。また、SnapCenterでは、バックアップとクローニングの処理に対応したスケジュールとポリシーの一元管理もサポートされます。

- 自動化された中央管理

日常的なSQL Serverバックアップのスケジュールを設定したり、ポリシーベースのバックアップ保持、ポイントインタイムのリストア処理、および最新の状態へのリストア処理を設定することができます。SnapCenterからのEメール アラートの送信を設定して、SQL Server環境をプロアクティブに監視することもできます。

- 無停止の**NetApp**スナップショットテクノロジー

Plug-in for SQL Serverは、NetApp SnapCenter Plug-in for Microsoft WindowsでNetApp Snapshotテクノロジーを使用します。これにより、データベースを数秒でバックアップし、SQL Serverをオフラインにすることなく迅速にリストアすることが可能です。Snapshotはストレージ スペースを最小限しか消費しません。

Plug-in for SQL Serverには、上記の主要な機能以外にも次のようなメリットがあります。

- バックアップ、リストア、クローニング、および検証のワークフローがサポートされます。

- セキュリティがRBACでサポートされ、ロール委譲が一元化されます。
- NetApp FlexCloneテクノロジーを使用して、テストまたはデータ抽出に使用する本番環境データベースのコピー（スペース効率に優れたポイントインタイム コピー）を作成できます。

クローンを保持するストレージ システムにFlexCloneライセンスが必要です。

- 自動化された無停止のバックアップ検証を利用できます。
- 複数のサーバで同時に複数のバックアップを実行できます。
- PowerShellコマンドレットを使用して、バックアップ、検証、リストア、クローニングの処理のスク립トを作成できます。
- SQL ServerのAlwaysOn可用性グループ（AG）をサポートしているため、AGのセットアップ、バックアップ、リストアの各処理を迅速に実行できます。
- SQL Server 2014の機能であるインメモリ データベースとバッファ プール拡張（BPE）がサポートされます。
- LUNと仮想マシン ディスク（VMDK）のバックアップがサポートされます。
- 物理インフラと仮想インフラがサポートされます。
- iSCSI、ファイバチャネル、FCoE、rawデバイス マッピング（RDM）、およびNFS / VMFS経由のVMDKがサポートされます。



NASボリュームに、Storage Virtual Machine（SVM）のデフォルト エクスポート ポリシーが必要です。

- SQL Serverのスタンドアロン データベースで、FileStreamとファイル グループがサポートされます。
- Windows Server 2022でNon-Volatile Memory express（NVMe）がサポートされます。
 - NVMe over TCP/IPで作成されたVMDKレイアウト上のバックアップ、リストア、クローニング、検証の各ワークフロー。
 - ESX 8.0 Update 2以降のNVMeファームウェア バージョン1.3をサポートします。仮想マシン ハードウェア バージョン21が必要です。
 - Windows Serverフェイルオーバー クラスタリング（WSFC）は、NVMe over TCP/IP上のVMDKを介したアプリケーションではサポートされません。
- サイト全体の障害時でもビジネス サービスの運用を継続できるようにするSnapMirrorアクティブ シンク（当初はSnapMirror Business Continuity [SM-BC] としてリリース）をサポートし、セカンダリ コピーを使用してアプリケーションを透過的にフェイルオーバーできるようにします。SnapMirrorアクティブ同期でフェイルオーバーをトリガーするために、手動操作や追加のスク립ト作成は必要ありません。

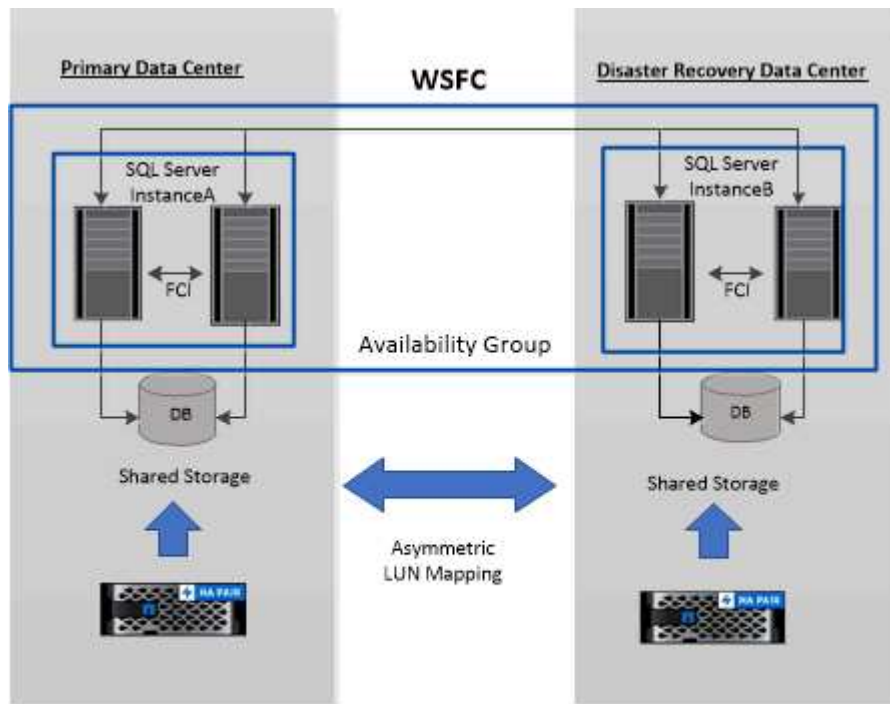
Windowsクラスタでの非対称LUNマッピングのサポート

SnapCenter Plug-in for Microsoft SQL Serverは、SQL Server 2012以降、高可用性のための非対称LUNマッピング（ALM）構成、およびディザスタ リカバリのための可用性グループの検出をサポートしています。リソースを検出する際、SnapCenter はALM 構成内のローカル ホストおよびリモート ホスト上のデータベースを検出します。

ALM構成は、プライマリ データセンターとディザスタ リカバリ データセンターそれぞれに1つ以上のノードを配置した、単一のWindows Serverフェイルオーバー クラスタです。

ALM構成の例を次に示します。

- マルチサイト データセンター内に2つのフェイルオーバー クラスタ インスタンス (FCI)
- ローカルの高可用性 (HA) をFCIで、ディザスタ リカバリ サイトに配置したスタンドアロン インスタンスによるディザスタ リカバリを可用性グループ (AG) で実現



WSFC-----Windows Server Failover Cluster

プライマリ データセンター内のストレージは、プライマリ データセンター内のFCIノード間で共有されます。ディザスタ リカバリ データセンター内のストレージは、ディザスタ リカバリ データセンター内のFCIノード間で共有されます。

プライマリ データセンターのストレージは、ディザスタ リカバリ データセンターのノードには認識されず、その逆も同様です。

ALMアーキテクチャは、FCIで使用する2つの共有ストレージ ソリューションと、SQL AGで使用する非共有（専用）ストレージ ソリューションを組み合わせたものです。AGソリューションは、データセンター間の共有ディスク リソースに同じドライブレターを使用します。クラスタ ディスクがWSFC内のノードのサブセット間で共有されるこのストレージ配置は、ALMと呼ばれます。

SnapCenter Plug-in for Microsoft SQL Serverでサポートされるストレージ タイプ

SnapCenterは、物理マシンと仮想マシンの両方でさまざまなストレージ タイプをサポートしています。ホストに対応したパッケージをインストールする前に、ストレージ タイプがサポートされているかどうかを確認する必要があります。

Windows Serverでは、SnapCenterによるプロビジョニングとデータ保護がサポートされます。サポートされているバージョンに関する最新情報について

は、[https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT\[\"NetApp Interoperability Matrix Tool\"\]](https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT[\)。

マシン	ストレージ タイプ	プロビジョニングを使用して	サポートノート
物理サーバ	FC接続LUN	SnapCenterのグラフィカル ユーザ インターフェイス (GUI) またはPowerShellコマンドレット	
物理サーバ	iSCSI接続LUN	SnapCenterのGUIまたはPowerShellコマンドレット	
物理サーバ	Storage Virtual Machine (SVM) 上のSMB3 (CIFS) 共有	SnapCenterのGUIまたはPowerShellコマンドレット	プロビジョニングのみがサポートされます。
VMware VM	FCまたはiSCSI HBAで接続されたRDM LUN	PowerShellコマンドレット	
VMware VM	iSCSIイニシエータでゲスト システムに直接接続されたiSCSI LUN	SnapCenterのGUIまたはPowerShellコマンドレット	
VMware VM	仮想マシン ファイルシステム (VMFS) またはNFSデータストア	VMware vSphere	
VMware VM	SVM上のSMB3共有に接続されたゲスト システム	SnapCenterのGUIまたはPowerShellコマンドレット	プロビジョニングのみがサポートされます。
VMware VM	NFSとSANの両方に存在するvVolデータストア	ONTAP Tools for VMware vSphere	

マシン	ストレージ タイプ	プロビジョニングを使用して	サポートノート
Hyper-V VM	仮想ファイバチャネル スイッチで接続された仮想FC (vFC) LUN	SnapCenterのGUIまたはPowerShellコマンドレット	仮想ファイバチャネル スイッチで接続された仮想FC (vFC) LUNのプロビジョニングには、Hyper-V Managerを使用する必要があります。  Hyper-Vのパススルーディスク、およびNetAppストレージでプロビジョニングされたVHD (VHDX) でのデータベースのバックアップはサポートされません。
Hyper-V VM	iSCSIイニシエータでゲスト システムに直接接続されたiSCSI LUN	SnapCenterのGUIまたはPowerShellコマンドレット	 Hyper-Vのパススルーディスク、およびNetAppストレージでプロビジョニングされたVHD (VHDX) でのデータベースのバックアップはサポートされません。

マシン	ストレージ タイプ	プロビジョニングを使用して	サポートノート
Hyper-V VM	SVM上のSMB3共有に接続されたゲスト システム	SnapCenterのGUIまたはPowerShellコマンドレット	プロビジョニングのみがサポートされます。  Hyper-Vのパススルーディスク、およびNetAppストレージでプロビジョニングされたVHD (VHDX) でのデータベースのバックアップはサポートされません。

SnapCenter Plug-in for Microsoft SQL Serverのストレージ レイアウトに関する推奨事項

ストレージ レイアウトが適切に設計されていると、SnapCenter Serverによるデータベースのバックアップでリカバリ目標を達成できます。ストレージ レイアウトを定義する際には、データベースのサイズ、データベースの変更率、バックアップの実行頻度など、いくつかの事項を考慮する必要があります。

以降のセクションで、SnapCenter Plug-in for Microsoft SQL Serverがインストールされている環境での、LUNと仮想マシン ディスク (VMDK) のストレージ レイアウトに関する推奨事項と制限について説明します。

この場合、LUNには、VMware RDMディスクや、ゲストにマッピングされたiSCSI直接接続型LUNを含めることができます。

LUNとVMDKの要件

次のデータベースのパフォーマンス最適化と管理のために、必要に応じて専用のLUNまたはVMDKを使用できます。

- マスター データベースとモデル システム データベース
- 一時データベース
- ユーザ データベース ファイル (.mdfおよび.ndf)
- ユーザ データベース トランザクション ログ ファイル (.ldf)
- ログ ディレクトリ

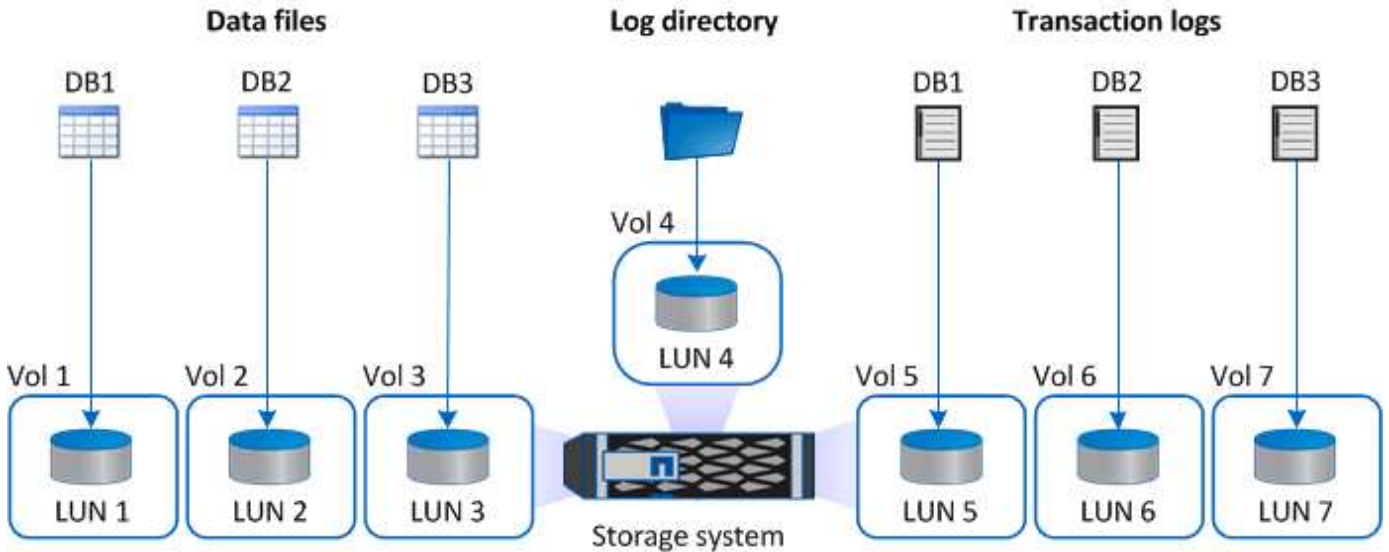
大規模なデータベースをリストアする場合は、専用のLUNまたはVMDKを使用することを推奨します。LUN全

体またはVMDK全体のリストアにかかる時間は、LUNまたはVMDKに格納されているファイルを個別にリストアするのにかかる時間よりも短くなります。

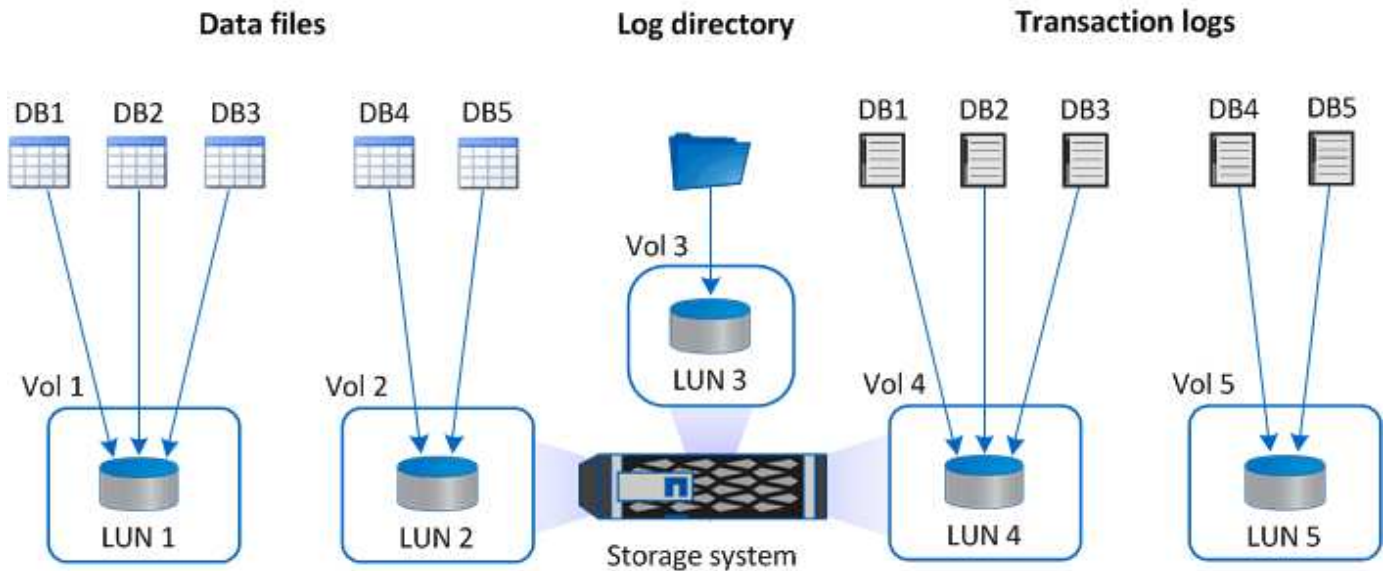
ログ ディレクトリについては、データ ディスクやログ ファイル ディスクに十分な空きスペースを確保するために、LUNまたはVMDKを別途作成する必要があります。

LUNおよびVMDKのサンプル レイアウト

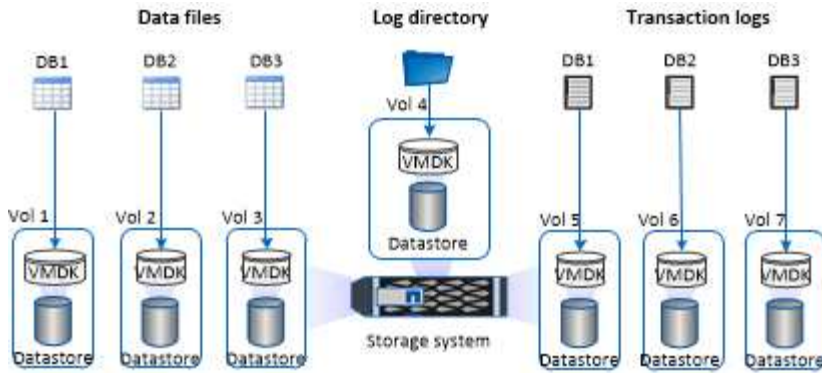
次の図は、LUN上に大規模データベースのストレージ レイアウトを構成する方法を示しています。



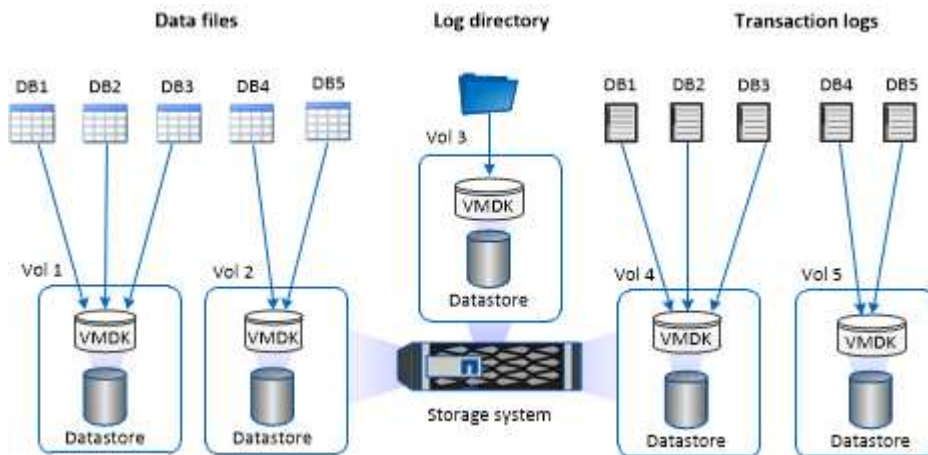
次の図は、LUN上に中規模または小規模データベースのストレージ レイアウトを構成する方法を示しています。



次の図は、VMDK上に大規模データベースのストレージ レイアウトを構成する方法を示しています。



次の図は、VMDK上に中規模または小規模データベースのストレージレイアウトを構成する方法を示しています。



SQLプラグインに必要な最小ONTAP権限

必要な最小ONTAP権限は、データ保護に使用するSnapCenterプラグインによって異なります。

- 全アクセス コマンド: ONTAP 9.12.1 以降に必要な最小限の権限
 - event generate-autosupport-log
 - job history show
 - job stop
 - lun
 - lun create
 - lun delete
 - lun igroup add
 - lun igroup create
 - lun igroup delete
 - lun igroup rename
 - lun igroup show
 - lun mapping add-reporting-nodes

- lun mapping create
- lun mapping delete
- lun mapping remove-reporting-nodes
- lun mapping show
- lun modify
- lun move-in-volume
- lun offline
- lun online
- lun resize
- lun serial
- lun show
- snapmirror policy add-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- snapmirror restore
- snapmirror show
- snapmirror show-history
- snapmirror update
- snapmirror update-ls-set
- snapmirror list-destinations
- version
- volume clone create
- volume clone show
- volume clone split start
- volume clone split stop
- volume create
- volume destroy
- volume file clone create
- volume file show-disk-usage
- volume offline
- volume online
- volume modify
- volume qtree create
- volume qtree delete
- volume qtree modify
- volume qtree show

- volume restrict
- volume show
- volume snapshot create
- volume snapshot delete
- volume snapshot modify
- volume snapshot rename
- volume snapshot restore
- volume snapshot restore-file
- volume snapshot show
- volume unmount
- vservers cifs
- vservers cifs share create
- vservers cifs share delete
- vservers cifs shadowcopy show
- vservers cifs share show
- vservers cifs show
- vservers export-policy
- vservers export-policy create
- vservers export-policy delete
- vservers export-policy rule create
- vservers export-policy rule show
- vservers export-policy show
- vservers iscsi
- vservers iscsi connection show
- vservers show
- ネットワークインターフェース
- network interface show
- SVM
- metrocluster show

Plug-in for SQL ServerのSnapMirrorレプリケーションとSnapVaultレプリケーション用のストレージ システムを準備する

SnapCenterプラグインと一緒にONTAP SnapMirrorテクノロジーを使用すると、バックアップセットのミラー コピーを別のボリュームに作成できます。また、ONTAP SnapVaultを使用すれば、標準への準拠やその他のガバナンスを目的としたディスクツォーディスクのバックアップ レプリケーションを実行できます。これらのタスクを実行する前に、ソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenterは、Snapshot処理の完了後に、SnapMirrorとSnapVaultに対する更新を実行します。SnapMirror更新とSnapVault更新は、SnapCenterジョブの一部として実行されるため、ONTAPスケジュールを別途作成しないでください。



NetApp SnapManager製品からSnapCenterに移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリ ストレージ（ソース ボリューム）上のデータがセカンダリ ストレージ（デスティネーション ボリューム）にレプリケートされます。この関係を初期化すると、ソース ボリュームで参照されるデータ ブロックがデスティネーション ボリュームに転送されます。



SnapCenter は、SnapMirrorとSnapVaultボリューム間のカスケード関係をサポートしていません（* プライマリ * > ミラー > ボールト）。ファンアウト関係を使用する必要があります。

SnapCenterは、バージョンに依存しないSnapMirror関係の管理をサポートしています。バージョンに依存しないSnapMirror関係とその設定方法の詳細については、["ONTAPのドキュメント"](#)。

SQL Serverリソースのバックアップ戦略

SQL Serverリソースのバックアップ戦略の定義

バックアップ ジョブを作成する前にバックアップ戦略を定義しておく、データベースの正常なリストアやクローニングに必要なバックアップを確実に作成できます。バックアップ戦略の大部分は、サービス レベル アグリーメント（SLA）、目標復旧時間（RTO）、および目標復旧時点（RPO）によって決まります。

SLAは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。RTOは、サービスの停止からビジネス プロセスの復旧までに必要となる時間です。RPOは、障害発生後に通常処理を再開するためにバックアップ ストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA、RTO、およびRPOは、バックアップ戦略に関与します。

サポートされるバックアップのタイプ

SnapCenterを使用してSQL Serverのシステム データベースとユーザ データベースをバックアップするには、リソース タイプ（データベース、SQL Serverインスタンス、可用性グループ[AG]など）を選択する必要があります。Snapshotテクノロジーを通じて、リソースが配置されているボリュームのオンラインの読み取り専用コピーが作成されます。

コピーのみのオプションを選択して、SQL Serverがトランザクション ログを切り捨てないように指定できます。SQL Serverの管理に他のバックアップ アプリケーションも使用している場合は、このオプションを指定する必要があります。トランザクション ログが変更されずに保持されるため、任意のバックアップ アプリケーションでデータベースをリストアできます。コピーのみのバックアップは、スケジュールされたバックアップとは関係なく実行され、またデータベースのバックアップおよびリストア手順には影響しません。

バックアップ タイプ	説明	コピーのみのオプションを選択した場合
フル バックアップとログ バックアップ	システム データベースがバックアップされ、トランザクション ログが切り捨てられます。 SQL Serverは、データベースにコミット済みのエントリを削除することによってトランザクション ログを切り捨てます。 このオプションを選択すると、フル バックアップの完了後にトランザクション ログが作成されてトランザクション情報がキャプチャされます。通常はこのオプションを選択します。ただし、バックアップ時間が短い場合は、フル バックアップでトランザクション ログ バックアップを実行しないように選択することもできます。 masterシステム データベースとmsdbシステム データベースについては、ログ バックアップを作成できません。modelシステム データベースのログ バックアップは作成できます。	システム データベース ファイルとトランザクション ログがバックアップされ、ログは切り捨てられません。 コピーのみのバックアップは差分ベースまたは差分バックアップとしては使用できず、差分ベースには影響しません。コピーのみのフル バックアップのリストアは、通常のフル バックアップのリストアと同じです。
フル データベース バックアップ	システム データベース ファイルがバックアップされます。 master、model、msdbの各システム データベースのフル データベース バックアップを作成できます。	システム データベース ファイルがバックアップされます。
トランザクション ログ バックアップ	切り捨てられたトランザクション ログがバックアップされ、最新のトランザクション ログのバックアップ後にコミットされたトランザクションのみがコピーされます。 フル データベース バックアップに加えてトランザクション ログを頻繁にバックアップするスケジュールを設定すると、リカバリ ポイントをより細かく選択できます。	トランザクション ログが切り捨てられずにバックアップされます。 このバックアップ タイプは、定期的なログ バックアップには影響しません。コピーのみのログ バックアップは、オンラインのリストア処理を実行する場合に便利です。

Plug-in for SQL Serverのバックアップ スケジュール

バックアップ頻度（スケジュール タイプ）はポリシーで指定され、バックアップ スケジ

ルールはリソース グループの設定で指定されます。バックアップの頻度またはスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率とデータの重要性です。使用頻度の高いリソースは1時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは1日に1回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービス レベル アグリーメント（SLA）、目標復旧時点（RPO）などがあります。

SLAは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。RPOは、障害発生後に通常処理を再開するためにバックアップストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLAとRPOはデータ保護戦略に関わる要件です。

使用頻度の高いリソースであっても、フル バックアップは1日に1～2回で十分です。たとえば、定期的なトランザクション ログ バックアップを実行すれば、必要なバックアップが作成されます。データベースを頻繁にバックアップするほど、SnapCenterが復元時に使用するトランザクション ログが少なくなり、復元操作が高速化されます。

バックアップ スケジュールには、次の2つの要素があります。

- バックアップ頻度

バックアップ頻度 (バックアップを実行する頻度) は、一部のプラグインでは スケジュール タイプ と呼ばれ、ポリシー構成の一部です。ポリシーでは、バックアップ頻度として、毎時、毎日、毎週、または毎月を選択できます。頻度を選択しなかった場合は、オンデマンドのみのポリシーが作成されます。設定 > ポリシー をクリックすると、ポリシーにアクセスできます。

- バックアップ スケジュール

バックアップ スケジュール (バックアップが実行される日時) は、リソース グループ設定の一部です。たとえば、週次バックアップのポリシーが構成されたリソース グループがある場合は、毎週木曜日の午後10 時にバックアップするようにスケジュールを構成できます。リソース > リソース グループ をクリックすると、リソース グループのスケジュールにアクセスできます。

データベースに必要なバックアップ ジョブの数

必要なバックアップ ジョブの数を左右する要因としては、データベースのサイズ、使用中のボリュームの数、データベースの変更率、サービス レベル アグリーメント（SLA）などがあります。

データベース バックアップの場合、選択するバックアップ ジョブの数は、一般にデータベースが配置されているボリュームの数に応じて決まります。たとえば、あるボリュームに小規模なデータベースのグループを配置しており、別のボリュームに1つの大規模なデータベースを配置している場合は、小規模なデータベース用のバックアップ ジョブと大規模なデータベース用のバックアップ ジョブを1つずつ作成できます。

Plug-in for SQL Serverのバックアップの命名規則

Snapshotのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則ではSnapshot名にタイムスタンプが追加されるので、コピーが作成されたタイミングを特定できます。

Snapshotでは、次のデフォルトの命名規則が使用されます。

resourcegroupname_hostname_timestamp

バックアップ リソース グループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- *dts1* はリソース グループ名です。
- *mach1x88* はホスト名です。
- *03-12-2015_23.17.26* は日付とタイムスタンプです。

または、[スナップショット コピーにカスタム名形式を使用する] を選択して、リソースまたはリソース グループを保護しながらスナップショット名の形式を指定することもできます。たとえば、*customtext_resourcegroup_policy_hostname*や*resourcegroup_hostname*などの形式です。デフォルトでは、Snapshot名にタイムスタンプのサフィックスが追加されます。

Plug-in for SQL Serverのバックアップ保持オプション

バックアップ コピーを保持する日数を選択するか、または保持するバックアップ コピーの数（ONTAPでは最大255個のコピー）を指定することができます。たとえば、組織の必要に応じて、10日分のバックアップ コピーや130個のバックアップ コピーを保持できます。

ポリシーを作成する際に、バックアップ タイプおよびスケジュール タイプの保持オプションを指定できます。

SnapMirrorレプリケーションを設定すると、デスティネーション ボリュームに保持ポリシーがミラーリングされます。

SnapCenter は、スケジュール タイプに一致する保持ラベルを持つ保持されたバックアップを削除します。リソースまたはリソース グループに対してスケジュール タイプが変更されると、古いスケジュール タイプ ラベルのバックアップがシステムに残ることがあります。



バックアップ コピーを長期にわたって保持する場合は、SnapVaultバックアップを使用する必要があります。

ソース ストレージ システムにトランザクション ログ バックアップを保持する期間

SnapCenter Plug-in for Microsoft SQL Serverでは、最新の状態へのリストア処理を実行するために、トランザクション ログ バックアップが必要です。この場合、2つのフル バックアップの間の任意の時点の状態にデータベースがリストアされます。

たとえば、Plug-in for SQL Server が午前 8 時に完全バックアップを実行し、午後 5 時にもう一度完全バックアップを実行した場合、最新のトランザクション ログ バックアップを使用して、データベースを午前 8 時から午後 5 時までの任意の時点に復元できます。トランザクション ログが使用できない場合、Plug-in for SQL

Server は、Plug-in for SQL Server が完全バックアップを完了した時点でデータベースを復元するポイントインタイム リストア操作のみを実行できます。

通常、最新の状態へのリストア処理に必要なのは1～2日分のみです。デフォルトでは、SnapCenterの保持期間は最短の2日間です。

同じボリューム上の複数のデータベース

バックアップ ポリシーには、バックアップあたりの最大データベース数を設定するオプション（デフォルト値は100）があるため、すべてのデータベースを同じボリュームに配置できます。

たとえば、同じボリュームに200個のデータベースがある場合、100個のデータベースを含むSnapshotが2つ作成されます。

Plug-in for SQL Serverのプライマリ ストレージ ボリュームまたはセカンダリ ストレージ ボリュームを使用したバックアップ コピーの検証

プライマリ ストレージ ボリュームまたはSnapMirror / SnapVaultセカンダリ ストレージ ボリュームでバックアップ コピーを検証することができます。セカンダリ ストレージ ボリュームを使用して検証を行うと、プライマリ ストレージ ボリュームの負荷が軽減されます。

プライマリ ストレージ ボリュームまたはセカンダリ ストレージ ボリュームにあるバックアップを検証すると、すべてのプライマリSnapshotとセカンダリSnapshotが検証済みとマークされます。

SnapMirrorおよびSnapVaultセカンダリ ストレージ ボリューム上のバックアップ コピーを検証するには、SnapRestoreのライセンスが必要です。

検証ジョブをスケジュール設定するタイミング

SnapCenterでは、バックアップの作成直後にそのバックアップを検証できますが、その場合、バックアップ ジョブの所要時間が大幅に増加し、大量のリソースが必要となります。このため、通常は別のジョブであとから検証を行うようにスケジュールを設定することを推奨します。たとえば、毎日午後5時にデータベースをバックアップする場合、検証を1時間後の午後6時に実行するようにスケジュールできます。

同じ理由で、通常、バックアップを実行するたびにバックアップの検証を行う必要はありません。通常、バックアップの整合性を確保するには、バックアップよりも少ない頻度で定期的に検証を実行すれば十分です。1つの検証ジョブで複数のバックアップを同時に検証できます。

SQL Serverのリストア戦略

リストア処理のソースとデスティネーション

プライマリ ストレージまたはセカンダリ ストレージにあるバックアップ コピーからSQL Serverデータベースをリストアすることができます。元の場所だけでなく別のデスティネーションにもデータベースをリストアできるため、要件に合うデスティネーションを選択できます。

リストア処理のソース

データベースはプライマリ ストレージまたはセカンダリ ストレージからリストアできます。

リストア処理のデスティネーション

データベースはさまざまなデスティネーションにリストアできます。

デスティネーション	説明
元の場所	デフォルトでは、SnapCenterは同じSQL Serverインスタンスの同じ場所にデータベースをリストアします。
別の場所	同じホスト内の任意のSQL Serverインスタンス上の別の場所にデータベースをリストアできます。
元の場所または別の場所で別のデータベース名を使用	バックアップを作成したホスト上の任意のSQL Serverインスタンスに、別の名前でデータベースをリストアできます。



VMDK上のSQLデータベース（NFSデータストアとVMFSデータストア）については、複数のESXサーバにまたがる代替ホストへのリストアはサポートされていません。

SnapCenterでサポートされるSQL Server復旧モデル

各データベース タイプには、デフォルトで特定の復旧モデルが割り当てられます。SQL Serverデータベース管理者は、各データベースの復旧モデルを変更できます。

SnapCenterは、3種類のSQL Server復旧モデルをサポートしています。

- 単純復旧モデル

単純復旧モデルを使用する場合は、トランザクション ログをバックアップできません。

- 完全復旧モデル

完全復旧モデルを使用する場合は、障害発生前の状態にデータベースをリストアできます。

- 一括ログ復旧モデル

一括ログ復旧モデルを使用する場合は、ログに一括記録された処理を手動で再実行する必要があります。ログに一括記録された処理のコミット レコードを含むトランザクション ログがリストア前にバックアップされていない場合は、一括記録された処理を実行する必要があります。ログに一括記録された処理でデータベースに1,000万行が挿入され、トランザクション ログがバックアップされる前にデータベースで障害が発生した場合、リストアされたデータベースに挿入された行は反映されません。

リストア処理のタイプ

SnapCenter を使用して、SQL Server リソースに対してさまざまな種類の復元操作を実

行できます。

- 最新の状態へのリストア
- 過去のある時点（ポイントインタイム）へのリストア

最新の状態または過去のある時点にリストアできるケースは次のとおりです。

- SnapMirrorまたはSnapVaultセカンダリ ストレージからリストアする
- 別のパス（場所）にリストアする



SnapCenterでは、ボリュームベースのSnapRestoreはサポートされません。

最新の状態へのリストア

最新の状態へのリストア処理（デフォルト）では、障害発生時点までデータベースがリカバリされます。SnapCenterでは、この処理が次の順序で実行されます。

1. データベースをリストアする前に、最後のアクティブなトランザクション ログがバックアップされます。
2. 選択したフル データベース バックアップからデータベースがリストアされます。
3. データベースにコミットされていないすべてのトランザクション ログが適用されます（バックアップ作成時から現時点までのバックアップのトランザクション ログを含む）。

トランザクション ログは再生されて選択したすべてのデータベースに適用されます。

最新の状態へのリストア処理を実行するには、連続したトランザクション ログ セットが必要です。

SnapCenter は、ログ配布バックアップ ファイルから SQL Server データベースのトランザクション ログを復元できないため (ログ配布を使用すると、プライマリ サーバー インスタンス上のプライマリ データベースから別のセカンダリ サーバー インスタンス上の 1 つ以上のセカンダリ データベースにトランザクション ログ バックアップを自動的に送信できます)、トランザクション ログ バックアップから最新の状態への復元操作を実行することはできません。このため、SQL Server データベースのトランザクション ログ ファイルをバックアップするには、SnapCenterを使用する必要があります。

すべてのバックアップに最新の状態へのリストア機能を使用する必要がない場合は、バックアップ ポリシーを使用してシステムのトランザクション ログ バックアップ保持を設定できます。

最新の状態へのリストア処理の例

毎日正午に SQL Server のバックアップを実行し、水曜日の午後 4 時にバックアップから復元する必要があるとします。何らかの理由により、水曜日の正午のバックアップの検証に失敗したため、火曜日の正午のバックアップを使用してリストアを実行することになりました。その後、バックアップが復元されると、火曜日のバックアップを作成した際にコミットされなかったトランザクション ログから始まり、水曜日の午後 4 時に書き込まれた最新のトランザクション ログまで (トランザクション ログがバックアップされている場合)、すべてのトランザクション ログが前へ移動され、復元されたデータベースに適用されます。

過去のある時点（ポイントインタイム）へのリストア

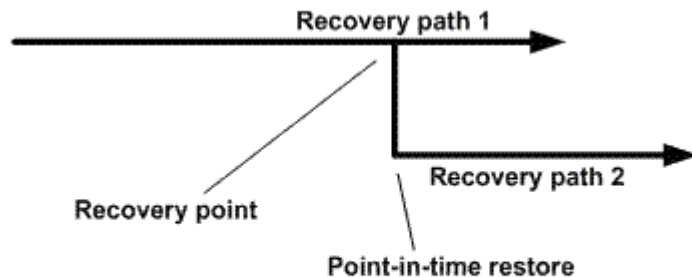
ポイントインタイム リストア処理では、データベースが過去の特定の時点にリストアされます。ポイントインタイム リストア処理は次の状況で発生します。

- バックアップ トランザクション ログの所定の時点までデータベースがリストアされた。
- データベースがリストアされ、一部のバックアップ トランザクション ログだけが適用された。



データベースをある時点までリストアすると、新しいリカバリ パスが発生します。

次の図は、ポイントインタイム リストア処理を実行した場合の問題を示しています。



この図のリカバリ パス1では、フル バックアップが作成され、その後複数のトランザクション ログ バックアップが作成されます。データベースをある時点にリストアします。ポイントインタイム リストア処理のあと、新しいトランザクション ログ バックアップが作成されて、リカバリ パス2が発生します。新しいトランザクション ログ バックアップが作成されるときに、新しいフル バックアップは作成されません。新しいフル バックアップが作成されるまでの間は、データ破損やその他の問題が発生しても現在のデータベースをリストアできません。また、リカバリ パス2で作成されたトランザクション ログを、リカバリ パス1のフル バックアップに適用することはできません。

トランザクション ログ バックアップ セットを適用する場合は、トランザクションの適用を終了する日時を指定することもできます。これを行うには、使用可能な範囲内で日付と時刻を指定すると、SnapCenter はその時点より前にコミットされていないトランザクションを削除します。この方法を使用すると、破損が発生する前の時点にデータベースをリストアしたり、誤って削除したデータベースやテーブルをリカバリしたりすることができます。

ポイントインタイム リストア処理の例

フル データベース バックアップを午前0時に1回、トランザクション ログ バックアップを1時間おきに実行しているとします。データベースは午前 9 時 45 分にクラッシュしましたが、障害が発生したデータベースのトランザクション ログをバックアップします。この場合、次に示すポイントインタイム リストアのシナリオが考えられます。

- 午前0時に作成されたフル データベース バックアップをリストアし、それ以後のデータベース変更については復元をあきらめる。（オプション：なし）
- 完全なデータベースバックアップを復元し、午前9時45分までのすべてのトランザクションログバックアップを適用します（オプション：ログの記録期限）
- フル データベース バックアップをリストアし、最後のトランザクション ログ バックアップ セットからリストアするトランザクションの時刻を指定して、トランザクション ログ バックアップを適用する。（オプション：特定の時間）

この場合は、エラーが報告された日時を特定します。指定した日時までにコミットされていなかったトランザクションすべては削除されます。

SQL Serverのクローニング戦略の定義

クローニング戦略を定義しておく、それに従ってデータベースのクローニングを実行することができます。

1. クローニング処理に関連する制限事項を確認します。
2. 必要なクローンのタイプを決定します。

クローニング処理の制限事項

データベースをクローニングする前に、クローニング処理の制限事項を確認しておく必要があります。

- Oracle の 11.2.0.4 から 12.1.0.1 までのバージョンを使用している場合、*renamedg* コマンドを実行するとクローン操作がハング状態になります。この問題を修正するには、Oracleパッチ19544733を適用します。
- (WindowsホストでMicrosoft iSCSIイニシエータを使用するなどして) ホストに直接接続されているLUNから、同じWindowsホスト上のVMDKかRDM LUN、または別のWindowsホストにデータベースをクローニングすることはできません。その逆も同様です。
- ボリューム マウント ポイントのルート ディレクトリを共有ディレクトリにすることはできません。
- クローンを含むLUNを新しいボリュームに移動すると、そのクローンは削除できなくなります。

クローニング処理のタイプ

SnapCenterを使用して、SQL Serverデータベースのバックアップまたは本番環境のデータベースをクローニングすることができます。

- データベース バックアップからのクローニング

クローンされたデータベースは、新しいアプリケーションを開発するためのベースラインとして機能し、運用環境で発生するアプリケーション エラーを分離するのに役立ちます。クローンされたデータベースは、ソフト データベース エラーからの回復にも使用できます。

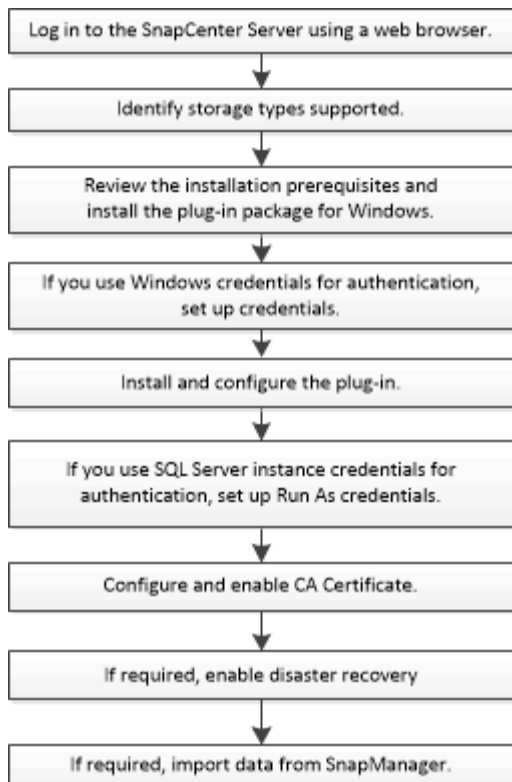
- クローンのライフサイクル

SnapCenter を使用すると、実稼働データベースがビジーでないときに実行される定期的なクローン ジョブをスケジュールできます。

SnapCenter Plug-in for Microsoft SQL Serverのインストール準備

SnapCenter Plug-in for Microsoft SQL Serverのインストール ワークフロー

SQL Server データベースを保護する場合は、Microsoft SQL Server 用のSnapCenterプラグインをインストールして設定する必要があります。



ホストを追加して**SnapCenter Plug-in for Microsoft SQL Server**をインストールするための前提条件

ホストを追加してプラグイン パッケージをインストールする前に、すべての要件を満たしておく必要があります。

- iSCSIを使用している場合は、iSCSIサービスが実行されている必要があります。
- ローカル管理者権限があり、リモート ホストに対するローカルのログイン アクセス許可があるユーザが必要です。
- SnapCenterでクラスタ ノードを管理する場合は、クラスタ内のすべてのノードに対する管理者権限があるユーザが必要です。
- SQL Serverに対するsysadminアクセス許可があるユーザが必要です。

SnapCenterプラグイン (Microsoft SQL Server 用) は、sysadmin アクセスを必要とする Microsoft VDI Framework を使用します。

["Microsoft サポート記事 2926557: SQL Server VDI のバックアップと復元操作には Sysadmin 権限が必要です"](#)

- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。
- SnapManager for Microsoft SQL Server がインストールされている場合は、サービスとスケジュールを停止または無効にする必要があります。

バックアップ ジョブまたはクローン ジョブをSnapCenterにインポートする予定の場合は、SnapManager for Microsoft SQL Server をアンインストールしないでください。

- サーバからホストを完全修飾ドメイン名（FQDN）に解決できる必要があります。

ホストファイルが解決可能になるように変更され、ホストファイルで短縮名とFQDNの両方が指定されている場合は、SnapCenterホストファイルに次の形式でエントリを作成します: <ip_address> <host_fqdn> <host_name>

SnapCenter Plug-ins Package for Windowsをインストールするホストの要件

SnapCenter Plug-ins Package for Windowsをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	Microsoft Windows サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	5 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK Java 11 Oracle Java および OpenJDK は、SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp対応プラグイン、および Windows ホストにインストールできるその他のカスタム アプリケーションにのみ必要です。 サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。

SnapCenter Plug-ins Package for Windowsのクレデンシャルの設定

SnapCenterは、クレデンシャルを使用してSnapCenterの処理を実行するユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、データベースやWindowsファイルシステムでのデータ保護処理に使用するクレデンシャルをそれぞれ作成する必要があります。

開始する前に

- プラグインのインストール前にWindowsクレデンシャルを設定する必要があります。
- このクレデンシャルには、管理者権限（リモート ホストに対する管理者権限を含む）を設定する必要があります。
- WindowsホストでのSQL認証

プラグインのインストール後にSQLクレデンシャルを設定する必要があります。

SnapCenter Plug-in for Microsoft SQL Serverを導入する場合は、プラグインのインストール後にSQLクレデンシャルを設定する必要があります。このクレデンシャルは、SQL Serverのsysadmin権限があるユーザに対して設定します。

SQL認証方式は、SQL Serverインスタンスに照らして認証します。したがって、SQL ServerインスタンスがSnapCenterで検出されなければなりません。そのため、SQLクレデンシャルを追加する前に、ホストの追加とプラグイン パッケージのインストールを完了し、リソースをリフレッシュしておく必要があります。SQL Server認証は、スケジュール設定やリソース検出などの処理を実行する際に必要になります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[資格情報]をクリックします。
3. *新規*をクリックします。
4. [Credential]ページで、クレデンシャルの設定に必要な情報を指定します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。

フィールド	操作
ユーザー名/パスワード	認証に使用するユーザ名とパスワードを入力します。 - ドメイン管理者 SnapCenterプラグインをインストールするシステムのドメイン管理者を指定します。[Username]フィールドの有効な形式は次のとおりです。 - NetBIOS\UserName - Domain FQDN\UserName - ローカル管理者（ワークグループの場合のみ） ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。ユーザー名フィールドの有効な形式は次のとおりです。 UserName パスワードには二重引用符 (") やバッククォート (') を使用しないでください。未満記号 (<) と感嘆符 (!) を組み合わせて使用したりしないでください。たとえば、lessthan<!10、lessthan10<!、バックティック`12 などです。
Authentication Mode	使用する認証モードを選択します。SQL認証モードを選択した場合は、SQL ServerインスタンスとそのSQLインスタンスのホストも指定する必要があります。

5. [OK]をクリックします。

クレデンシャルの設定が完了したら、必要に応じて[User and Access]ページでユーザやユーザ グループにクレデンシャルを割り当てることができます。

個々のSQL Serverリソースのクレデンシャルの設定

各ユーザについて、個々のSQL Serverリソースに対してデータ保護ジョブを実行するためのクレデンシャルを設定できます。クレデンシャルはグローバルに設定することもできますが、必要に応じて特定のリソースに対してのみ設定することもできます。

タスク概要

- Windowsクレデンシャルを認証に使用している場合は、プラグインのインストール前にクレデンシャルを設定する必要があります。

一方、SQL Serverインスタンスを認証に使用している場合は、プラグインのインストール後にクレデンシャルを追加する必要があります。

- クレデンシャルの設定時にSQL認証を有効にすると、検出されたインスタンスやデータベースに赤い鍵マークのアイコンが表示されます。

鍵マークのアイコンが表示されている場合、リソース グループに追加する際にそのインスタンスまたはデータベースのクレデンシャルを指定する必要があります。

- 次の条件に該当する場合、sysadminアクセスがないロールベース アクセス制御（RBAC）ユーザにクレデンシャルを割り当てる必要があります。
 - SQLインスタンスにクレデンシャルが割り当てられている。
 - SQLインスタンスまたはホストがRBACユーザに割り当てられている。

ユーザには、リソース グループとバックアップの両方の権限が必要です。

ステップ1: 資格情報を追加して構成する

- 左側のナビゲーション ペインで、[設定] を選択します。
- 設定ページで、*資格情報*を選択します。
 - 新しい資格情報を追加するには、[新規] を選択します。
 - [Credential] ページでクレデンシャルを設定します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。
ユーザー名	SQL Server認証に使用するユーザ名を入力します。 - ドメイン管理者または管理者グループのメンバーSnapCenterプラグインをインストールするシステムのドメイン管理者または管理者グループのメンバーを指定します。*ユーザー名*フィールドの有効な形式は次のとおりです。 - NetBIOS\ユーザー名 - ドメインFQDN\ユーザー名 - ローカル管理者（ワークグループのみ） ワークグループに属するシステムの場合は、 SnapCenterプラグインをインストールするシステムに組み込まれているローカル管理者を指定します。ユーザーアカウントに昇格された権限が付与されている場合、またはホストシステムでユーザーアクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカルユーザーアカウントを指定できます。 *ユーザー名*フィールドの有効な形式は次のとおりです: <i>UserName</i>

フィールド	操作
パスワード	認証に使用するパスワードを入力します。
認証モード	SQL Server認証モードを選択します。SQL Serverに対するsysadmin権限があるWindowsユーザの場合は、Windows認証を選択することもできます。
ホスト	ホストを選択します。
SQL Server インスタンス	SQL Serverインスタンスを選択します。

c. 資格情報を追加するには、[OK] を選択します。

ステップ2: インスタンスを構成する

1. 左側のナビゲーション ペインで、[リソース] を選択します。
2. [リソース] ページで、[表示] リストから [インスタンス] を選択します。
 - a. image:.../media/filter_icon.png[フィルター アイコン]を選択し、ホスト名を選択してインスタンスをフィルターします。
 - b. フィルター パネルを閉じるには、image:.../media/filter_icon.png[フィルター アイコン] を選択します。
3. 「インスタンス保護」 ページでインスタンスを保護し、必要に応じて「資格情報の構成」を選択します。

SnapCenter ServerにログインしているユーザにSnapCenter Plug-in for Microsoft SQL Serverへのアクセス権がない場合、そのユーザはクレデンシャルを設定する必要があります。



クレデンシャル オプションは、データベースおよび可用性グループには適用されません。

4. *リソースの更新*を選択します。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、作成したグループ管理サービス アカウント (gMSA) を通じて、管理対象ドメイン アカウントからサービス アカウントのパスワードを自動管理できます。

開始する前に

- Windows Server 2016以降のドメイン コントローラが必要です。
- ドメインのメンバーであるWindows Server 2016以降のホストが必要です。

手順

1. KDSルート キーを作成し、gMSA内のオブジェクトごとに一意のパスワードを生成します。
2. 各ドメインについて、Windowsドメインコントローラから次のコマンドを実行します: Add-KDSRootKey -Effectivelmmmediately

3. gMSAを作成して設定します。

- a. 次の形式でユーザ グループ アカウントを作成します。

```
domainName\accountName$  
.. コンピュータ オブジェクトをグループに追加します。  
.. 作成したユーザ グループを使用してgMSAを作成します。
```

次に例を示します。

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 走る `Get-ADServiceAccount` サービス アカウントを確認するコマンド。
```

4. ホストでgMSAを設定します。

- a. gMSAアカウントを使用するホストで、Windows PowerShell用のActive Directoryモジュールを有効にします。

これを行うには、PowerShellから次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. ホストを再起動します。
- b. PowerShell コマンド プロンプトから次のコマンドを実行して、ホストに gMSA をインストールします。 `Install-AdServiceAccount <gMSA>`
- c. 次のコマンドを実行して、gMSA アカウントを確認します。 `Test-AdServiceAccount <gMSA>`

5. ホスト上の設定済みgMSAに管理者権限を割り当てます。
6. SnapCenter Serverで設定済みのgMSAアカウントを指定してWindowsホストを追加します。

SnapCenter Serverにより、選択したプラグインがホストにインストールされ、プラグインのインストール時には指定したgMSAがサービスのログオン アカウントとして使用されます。

SnapCenter Plug-in for Microsoft SQL Serverのインストール

ホストの追加とSnapCenter Plug-ins Package for Windowsのインストール

ホストを追加し、プラグイン パッケージをインストールするには、SnapCenter の*ホストの追加* ページを使用する必要があります。プラグインは、自動的にリモート ホストにインストールされます。

開始する前に

- SnapCenter Serverホストのオペレーティング システムがWindows 2019で、プラグイン ホストのオペレーティング システムがWindows 2022の場合は、次の手順を実行する必要があります。
 - Windows Server 2019（OSビルド17763.5936）以降にアップグレードする
 - Windows Server 2022（OSビルド20348.2402）以降にアップグレードする
- この処理は、SnapCenter Adminロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。
- 組み込みでないクレデンシャルを指定してWindowsホストにプラグインをインストールする場合は、ホストのUACを無効にする必要があります。
- メッセージ キュー サービスが実行中であることを確認する必要があります。
- グループ管理サービス アカウント（gMSA）を使用する場合は、管理者権限でgMSAを設定する必要があります。

["Windows Server 2016 以降で SQL 用のグループ管理サービス アカウントを構成する"](#)

タスク概要

SnapCenter Serverをプラグイン ホストとして別のSnapCenter Serverに追加することはできません。

ホストの追加とプラグイン パッケージのインストールは、ホストごとまたはクラスタごとに実行できます。クラスタまたはWindows Serverフェイルオーバー クラスターリング（WSFC）にプラグインをインストールする場合、プラグインはクラスタのすべてのノードにインストールされます。

ホストの管理については、以下を参照してください。 ["ホストの管理"](#)。

手順

1. 左側のナビゲーション ペインで、[ホスト] を選択します。
2. 上部の*管理対象ホスト*タブが選択されていることを確認します。
3. *追加*を選択します。
4. [Hosts]ページで次の操作を実行します。

フィールド	操作
ホストタイプ	ホスト タイプとして[Windows]を選択します。SnapCenter Serverはホストを追加し、Plug-in for Windowsをホストにインストールします（プラグインがまだインストールされていない場合）。 [Plug-ins]ページで[Microsoft SQL Server]オプションを選択した場合、SnapCenter ServerはPlug-in for SQL Serverをインストールします。
ホスト名	ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。信頼されないドメイン ホストのIPアドレスは、FQDNに解決される場合にのみサポートされます。 SnapCenterが機能するためには、DNSが適切に設定されている必要があります。そのため、FQDNを入力することを推奨します。 次のいずれかのIPアドレスまたはFQDNを入力できます。 • スタンドアロン ホスト • WSFC SnapCenterを使用してホストを追加し、そのホストがサブドメインの一部である場合は、FQDN を指定する必要があります。
Credentials	作成したクレデンシャル名を選択するか、新しいクレデンシャルを作成します。このクレデンシャルには、リモート ホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 指定したクレデンシャル名にカーソルを合わせると、クレデンシャルの詳細を確認できます。  クレデンシャルの認証モードは、[Add Host]ウィザードで指定するホスト タイプによって決まります。

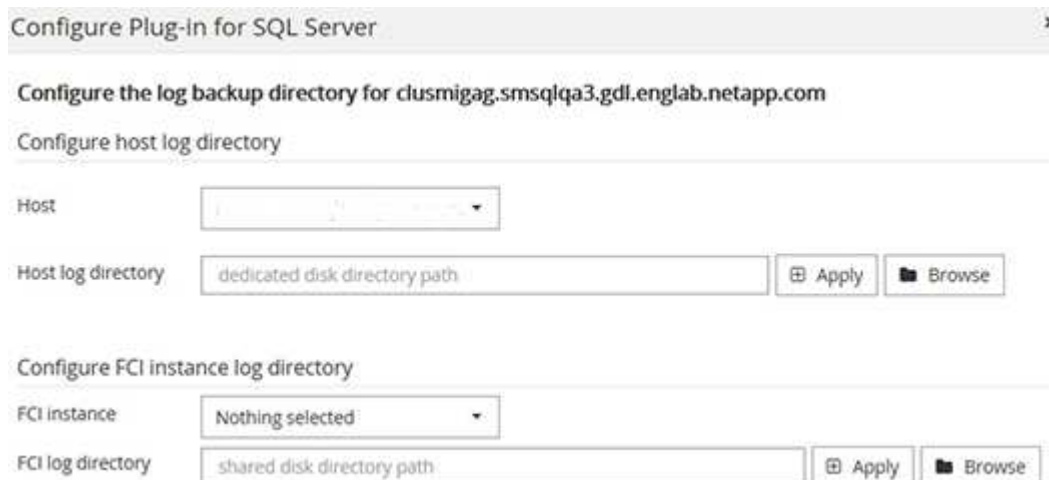
5. *インストールするプラグインの選択*セクションで、インストールするプラグインを選択します。

6. *その他のオプション*を選択します。

フィールド	操作
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。デフォルトのポート番号は8145です。SnapCenter Serverがカスタム ポートにインストールされている場合は、そのポート番号がデフォルト ポートとして表示されます。  プラグインを手動でインストールしてカスタム ポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理が失敗します。
Installation Path	デフォルトのパスはC:\Program Files\NetApp\SnapCenterです。必要に応じて変更できます。
クラスター内のすべてのホストを追加する	WSFCまたはSQL可用性グループ内のすべてのクラスタ ノードを追加するには、このチェック ボックスをオンにします。クラスター内の使用可能な複数のSQL可用性グループを管理および識別する場合は、GUIで該当するクラスタのチェック ボックスをオンにして、すべてのクラスタ ノードを追加する必要があります。
Skip preinstall checks	プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェック ボックスをオンにします。
Use group Managed Service Account (gMSA) to run the plug-in services	グループ管理サービス アカウント (gMSA) を使用してプラグイン サービスを実行する場合は、このチェック ボックスをオンにします。 gMSA名をdomainName\accountName\$の形式で指定します。  ホストがgMSAに追加されていて、gMSAにログイン権限とシステム管理者権限がある場合は、SQLインスタンスへの接続にgMSAが使用されます。

7. *送信*を選択します。
8. (SQLプラグインの場合) ログ ディレクトリを設定するホストを選択します。
 - a. ログ ディレクトリの構成 を選択し、ホスト ログ ディレクトリの構成ページで 参照 を選択して、次の手順を実行します。

NetApp LUN（ドライブ）のみが選択肢として表示されます。SnapCenterは、バックアップ処理の一環として、ホスト ログ ディレクトリをバックアップしてレプリケートします。



- i. ホスト ログの格納先とするホスト上のドライブ レターまたはマウント ポイントを選択します。
 - ii. 必要に応じてサブディレクトリを選択します。
 - iii. *保存*を選択します。
9. *送信*を選択します。

「事前チェックをスキップ」チェックボックスを選択していない場合、ホストがプラグインのインストール要件を満たしているかどうかを検証されます。ディスク容量、RAM、PowerShellバージョン、.NETバージョン、場所（Windowsプラグインの場合）、Javaバージョン（Linuxプラグインの場合）が最小要件に照らして検証されます。最小要件を満たしていない場合、対応するエラーまたは警告メッセージが表示されます。

エラーがディスク スペースまたはRAMに関連している場合は、C:\Program Files\NetApp\SnapCenter WebAppにあるweb.configファイルを更新してデフォルト値を変更できます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。



HAのセットアップでweb.configファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

10. インストールの進捗状況を監視します。

コマンドレットを使用した複数のリモート ホストへの**SnapCenter Plug-in for Microsoft SQL Server**のインストール

PowerShellのInstall-SmHostPackageコマンドレットを使用すると、SnapCenter Plug-in for Microsoft SQL Serverを複数のホストに同時にインストールできます。

開始する前に

プラグイン パッケージをインストールする各ホストに対するローカル管理者権限を持つドメイン ユーザとして、SnapCenterにログインしておく必要があります。

手順

1. PowerShellを起動します。

2. SnapCenter Serverホストで、Open-SmConnectionコマンドレットを使用してセッションを確立し、クレデンシャルを入力します。
3. Install-SmHostPackageコマンドレットと必要なパラメータを使用して、複数のリモート ホストにSnapCenter Plug-in for Microsoft SQL Serverをインストールします。

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、-skipprcheckオプションを使用できます。

4. リモート インストールのクレデンシャルを入力します。

コマンドラインからの**SnapCenter Plug-in for Microsoft SQL Server**のサイレント インストール

SnapCenter Plug-in for Microsoft SQL Serverは、SnapCenterユーザ インターフェイス内からインストールする必要があります。ただし、何らかの理由でインストールできない場合は、Windowsのコマンドラインから、Plug-in for SQL Serverのインストール プログラムをサイレント モードで自動的に実行できます。

開始する前に

- インストール前に、以前のバージョンのSnapCenter Plug-in for Microsoft SQL Serverを削除する必要があります。

詳細については、以下を参照してください。"[SnapCenterプラグインをプラグインホストから手動で直接インストールする方法](#)"。

手順

1. プラグイン ホストにC:\tempフォルダが存在するかどうか、およびログインしているユーザにそのフォルダへのフル アクセス権があるかどうかを確認します。
2. Plug-in for SQL ServerソフトウェアをC:\ProgramData\NetApp\SnapCenter\Packageリポジトリからダウンロードします。

このパスには、SnapCenter Serverがインストールされているホストからアクセスできます。

3. プラグインをインストールするホストにインストール ファイルをコピーします。
4. ローカル ホストのWindowsコマンド プロンプトで、プラグインのインストール ファイルを保存したディレクトリに移動します。
5. Plug-in for SQL Serverソフトウェアをインストールします。

```
"snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"  
/log"Log_Path" BI_SNAPCENTER_PORT=Num  
SUITE_INSTALLDIR="Install_Directory_Path"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW,SCSQL
```

プレースホルダの値をユーザ自身のデータに置き換えます。

- Debug_Log_Path は、スイート インストーラー ログ ファイルの名前と場所です。
- Log_Path は、プラグイン コンポーネント (SCW、SCSQL、および SMCore) のインストール ログの場所です。
- NumはSnapCenterがSMCoreと通信するポートです
- Install_Directory_Path は、ホスト プラグイン パッケージのインストール ディレクトリです。
- domain\administrator は、 SnapCenter Plug-in for Microsoft Windows Web サービス アカウントです。
- password は、 SnapCenter Plug-in for Microsoft Windows Web サービス アカウントのパスワードです。+

```
"snapcenter_windows_host_plugin.exe"/silent
/debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\ " BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW,SCSQL
```



Plug-in for SQL Serverのインストール時に渡されるすべてのパラメータでは、大文字と小文字が区別されます。

6. Windowsタスク スケジューラ、メイン インストール ログ ファイルのC:\ Installdebug.log、C:\Temp内の追加のインストール ファイルを監視します。
7. %temp%ディレクトリを監視して、msiexe.exeインストーラがエラーなくソフトウェアをインストールしていることを確認します。



Plug-in for SQL Serverをインストールすると、SnapCenter Serverではなくホストにプラグインが登録されます。SnapCenter GUIまたはPowerShellコマンドレットを使用してホストを追加することにより、SnapCenter Serverにプラグインを登録できます。ホストを追加すると、プラグインが自動的に検出されます。

Plug-in for SQL Serverのインストール ステータスの監視

[Jobs]ページを使用して、SnapCenterプラグイン パッケージのインストールの進捗状況を監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター* ページで、*ジョブ* をクリックします。
3. ジョブ ページで、プラグインのインストール操作のみがリストされるようにリストをフィルタリングするには、次の手順を実行します。
 - a. *フィルター* をクリックします。
 - b. オプション：開始日と終了日を指定します。
 - c. [タイプ] ドロップダウン メニューから、[プラグインのインストール] を選択します。
 - d. [Status] ドロップダウン メニューから、インストールのステータスを選択します。
 - e. *適用* をクリックします。
4. インストール ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細* ページで、*ログの表示* をクリックします。

CA 証明書の設定

CA 証明書 CSR ファイルの生成

証明書署名要求 (CSR) を生成し、生成した CSR を使用して認証局 (CA) から取得した証明書をインポートできます。証明書には秘密キーが関連付けられます。

CSR はエンコードされたテキストのブロックであり、署名済み CA 証明書を取得するために認定証明書ベンダーに提供されます。



CA 証明書の RSA キーの長さは最低 3072 ビットである必要があります。

CSR を生成するための情報については、["CA 証明書 CSR ファイルの生成方法"](#)。



ドメイン (*.domain.company.com) またはシステム (machine1.domain.company.com) の CA 証明書を所有している場合は、CA 証明書 CSR ファイルの生成をスキップできます。SnapCenter を使用して、既存の CA 証明書を導入できます。

クラスタ構成の場合、クラスタ名 (仮想クラスタ FQDN) と、それぞれのホスト名が CA 証明書に記載されている必要があります。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。ワイルドカード証明書 (*.domain.company.com) の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA 証明書のインポート

Microsoft 管理コンソール (MMC) を使用して、SnapCenter Server と Windows ホスト プラグインに CA 証明書をインポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。

3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
4. コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書 をクリックします。
5. 「信頼されたルート証明機関」フォルダを右クリックし、[すべてのタスク] > [インポート] を選択して、インポート ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*次へ*をクリックします。
インポート ファイル形式	変更せずに、[次へ] をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、[次へ] をクリックします。
証明書のインポート ウィザードの完了	概要を確認し、[完了] をクリックしてインポートを開始します。



インポートする証明書は秘密キーとバンドルされている必要があります (サポートされている形式は **.pfx**、**.p12**、および ***.p7b** です)。

7. 「個人用」フォルダに対して手順5を繰り返します。

CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための16進数の文字列です。サムプリントは、サムプリント アルゴリズムを使用して証明書の内容から計算されます。

手順

1. GUIで次の手順を実行します。
 - a. 証明書をダブルクリックします。
 - b. [証明書] ダイアログボックスで、[詳細] タブをクリックします。
 - c. フィールドのリストをスクロールして、「拇印」をクリックします。
 - d. ボックスから16進数の文字をコピーします。
 - e. 16進数の間のスペースを削除します。

たとえば、拇印が「a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b」の場合、スペースを削除すると「a909502dd82ae41433e6f83886b00d4277a32a7b」になります。

2. PowerShellで、次の手順を実行します。
 - a. 次のコマンドを実行して、インストールされている証明書のサムプリントを表示し、最近インストー

ルされた証明書をサブジェクト名で識別します。

Get-ChildItem -Path 証明書:\LocalMachine\My

- b. サムプリントをコピーします。

Windowsホスト プラグイン サービスでのCA証明書の設定

インストールされているデジタル証明書をアクティブ化するには、Windowsホスト プラグイン サービスを使用してCA証明書を設定する必要があります。

SnapCenter Serverと、CA証明書がすでに導入されているすべてのプラグイン ホストで、次の手順を実行します。

手順

1. 次のコマンドを実行して、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例えば：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 次のコマンドを実行して、新しくインストールした証明書をWindowsホスト プラグイン
サービスとバインドします。
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例えば：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

プラグインのCA証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインでCA証明書の検証を有効にする必要があります。

開始する前に

- 実行 *Set-SmCertificateSettings* コマンドレットを使用して、CA 証明書を有効または無効にすることができます。

- `Get-SmCertificateSettings` を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. プラグイン ホストを1つまたは複数選択します。
4. *その他のオプション* をクリックします。
5. *証明書の検証を有効にする* を選択します。

終了後の操作

[Managed Hosts] タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Server とプラグイン ホスト間の接続のステータスを示します。

- *🔑* は、CA 証明書が有効になっていないか、プラグイン ホストに割り当てられていないことを示します。
- *🟢* は CA 証明書が正常に検証されたことを示します。
- *🔴* は、CA 証明書を検証できなかったことを示します。
- *🔒* は接続情報を取得できなかったことを示します。



ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

ディザスタ リカバリの設定

SnapCenter Plug-in for SQL Server のディザスタ リカバリ

SnapCenter Plug-in for SQL Server が停止した場合は、次の手順に従って別の SQL ホストに切り替え、データをリカバリします。

開始する前に

- セカンダリ ホストのオペレーティング システム、アプリケーション、ホスト名が、プライマリ ホストと同じである必要があります。
- ホストの追加 または ホストの変更 ページを使用して、SQL Server 用の SnapCenter プラグインを別のホストにプッシュします。見る "[ホストの管理](#)" 詳細についてはこちらをご覧ください。

手順

1. ホスト ページからホストを選択し、SQL Server 用の SnapCenter プラグインを変更してインストールします。
2. (オプション) SnapCenter Plug-in for SQL Server の構成ファイルを、ディザスタ リカバリ (DR) バックアップから新しいマシンに置き換えます。
3. Windows と SQL スケジュールを、DR バックアップの SnapCenter Plug-in for SQL Server フォルダからインポートします。

参照["災害復旧API"ビデオ](#)。

SnapCenter Plug-in for SQL Serverのストレージのディザスタ リカバリ (DR)

SnapCenter Plug-in for SQL Serverのストレージをリカバリするには、[Global Settings] ページでストレージのDRモードを有効にします。

開始する前に

- プラグインがメンテナンス モードであることを確認します。
- SnapMirror/ SnapVault関係を解除します。["SnapMirror関係の解除"](#)
- セカンダリのLUNを同じドライブ レターでホスト マシンに接続します。
- すべてのディスクが、DR前に使用していたのと同じドライブ レターで接続されていることを確認します。
- MSSQLサーバ サービスを再起動します。
- SQLリソースがオンラインに戻っていることを確認します。

タスク概要

VMDK構成およびRDM構成では、ディザスタ リカバリ (DR) はサポートされません。

手順

1. 設定ページで、設定 > グローバル設定 > *災害復旧*に移動します。
2. *災害復旧を有効にする*を選択します。
3. *適用*をクリックします。
4. モニター > ジョブ をクリックして、DR ジョブが有効になっているかどうかを確認します。

終了後の操作

- フェイルオーバー後に新しいデータベースが作成されると、データベースは非DRモードになります。

新しいデータベースは、フェイルオーバー前と同じように動作し続けます。

- DRモードで作成された新しいバックアップは、[Topology]ページの[SnapMirror]または[SnapVault (secondary)]に一覧表示されます。

新しいバックアップの横に、これらのバックアップがDRモード中に作成されたことを示す「i」のアイコンが表示されます。

- フェールオーバー中に作成されたSnapCenter Plug-in for SQL Server のバックアップは、UI または次のコマンドレットを使用して削除できます。 `Remove-SmBackup`
- フェイルオーバー後、一部のリソースを非 DR モードにする場合は、次のコマンドレットを使用します。 `Remove-SmResourceDRMode`

詳細については、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

- SnapCenter Serverは、ストレージ リソースがDRモードであるか非DRモードであるかにかかわらず、個々のストレージ リソース (SQLデータベース) を管理しますが、ストレージ リソースを含むリソース グ

ループは管理しません。

SnapCenter Plug-in for SQL Serverのセカンダリ ストレージからプライマリ ストレージへのフェイルバック

SnapCenter Plug-in for SQL Serverのプライマリ ストレージがオンラインに戻ったら、プライマリ ストレージにフェイルバックする必要があります。

開始する前に

- 管理対象ホスト ページから、SQL Server 用のSnapCenterプラグインを メンテナンス モードにします。
- セカンダリ ストレージをホストから切断し、プライマリ ストレージから接続します。
- プライマリ ストレージにフェイルバックするには、逆再同期処理を実行して、関係の方向がフェイルオーバー前と変わらないようにします。

逆再同期操作後にプライマリ ストレージとセカンダリ ストレージの役割を保持するには、逆再同期操作をもう一度実行します。

詳細については、"[ミラー関係の逆再同期](#)"

- MSSQLサーバ サービスを再起動します。
- SQLリソースがオンラインに戻っていることを確認します。



プラグインのフェイルオーバー中やフェイルバック中は、プラグインの全体的なステータスはすぐには更新されません。ホストとプラグインの全体的なステータスは、次のホスト更新処理で更新されます。

手順

1. 設定ページで、設定 > グローバル設定 > *災害復旧*に移動します。
2. *災害復旧を有効にする*の選択を解除します。
3. *適用*をクリックします。
4. モニター > ジョブ をクリックして、DR ジョブが有効になっているかどうかを確認します。

終了後の操作

フェールオーバー中に作成されたSnapCenter Plug-in for SQL Server のバックアップは、UI または次のコマンドレットを使用して削除できます。 `Remove-SmDRFailoverBackups`

SnapCenter Plug-in for VMware vSphereのインストール

データベースまたはファイルシステムが仮想マシン（VM）に格納されている場合や、VMとデータストアを保護する場合は、SnapCenter Plug-in for VMware vSphere仮想アプライアンスを導入する必要があります。

展開方法については、"[導入プロセスの概要](#)"。

CA証明書を導入する

SnapCenter Plug-in for VMware vSphereで CA 証明書を構成するには、以下を参照してください。"[SSL証明書を作成またはインポートする](#)"。

CRLファイルを設定する

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリでCRLファイルを探します。SnapCenter Plug-in for VMware vSphere のCRL ファイルのデフォルト ディレクトリは `/opt/netapp/config/crl` です。

このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

データ保護の準備

SnapCenter Plug-in for Microsoft SQL Serverを使用するための前提条件

ユーザがPlug-in for SQL Serverの使用を開始するためには、SnapCenter管理者が事前にSnapCenter Serverをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter Serverをインストールして設定します。
- SnapCenterにログインします。
- SnapCenter環境を設定するために、ストレージ システム接続の追加または割り当てを行い、クレデンシャルを作成します。



SnapCenterでは、別々のクラスタに属している場合でも、複数のSVMに同じ名前を付けることはサポートされません。SnapCenterでサポートするSVMには、すべて一意の名前を付ける必要があります。

- ホストを追加し、プラグインをインストールし、リソースを検出（更新）し、プラグインを設定します。
- `Invoke-SmConfigureResources`を実行し、既存のMicrosoft SQL Serverデータベースをローカル ディスクからNetApp LUNに（またはその逆）移動します。

コマンドレットの実行方法については、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"

- SnapCenter Serverを使用してVMware RDM LUNまたはVMDK上のSQLデータベースを保護する場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。詳細については、SnapCenter Plug-in for VMware vSphereのドキュメントを参照してください。

"[SnapCenter Plug-in for VMware vSphereのドキュメント](#)"

- SnapCenter Plug-in for Microsoft Windowsを使用して、ホスト側のストレージをプロビジョニングします。
- バックアップ レプリケーションが必要である場合は、SnapMirror関係とSnapVault関係をセットアップします。

詳細については、SnapCenterのインストールに関する説明を参照してください。

SnapCenter Plug-in for VMware vSphere 4.1.1のドキュメントには、SnapCenter 4.1.1のユーザ向けに、仮想データベースとファイルシステムの保護に関する情報が記載されています。NetApp Data Broker 1.0および1.0.1のドキュメントには、SnapCenter 4.2.xのユーザ向けに、LinuxベースのNetApp Data Broker仮想アプライアンス（オープン仮想アプライアンス形式）が提供するSnapCenter Plug-in for VMware vSphereを使用した仮想データベースとファイルシステムの保護に関する情報が記載されています。SnapCenter Plug-in for VMware vSphere 4.3のドキュメントには、SnapCenter 4.3.xのユーザ向けに、LinuxベースのSnapCenter Plug-in for VMware vSphere仮想アプライアンス（オープン仮想アプライアンス形式）を使用した仮想データベースとファイルシステムの保護に関する情報が記載されています。

"SnapCenter Plug-in for VMware vSphereのドキュメント"

SQL Serverの保護におけるソース、リソース グループ、ポリシーの使用方法

SnapCenterを使用する前に、実行するバックアップ、クローニング、リストアの各処理に関連する基本的な概念を理解しておく役立ちます。ここでは、これらの処理で扱うリソース、リソース グループ、およびポリシーについて説明します。

- リソースは通常、SnapCenterを使用してバックアップまたはクローンを作成するデータベース、データベース インスタンス、または Microsoft SQL Server 可用性グループです。
- SnapCenterリソース グループは、ホストまたはクラスタ上のリソースの集まりです。

リソース グループに対して処理を実行すると、リソース グループに指定したスケジュールに従って、リソース グループに定義されているリソースに対して処理が実行されます。

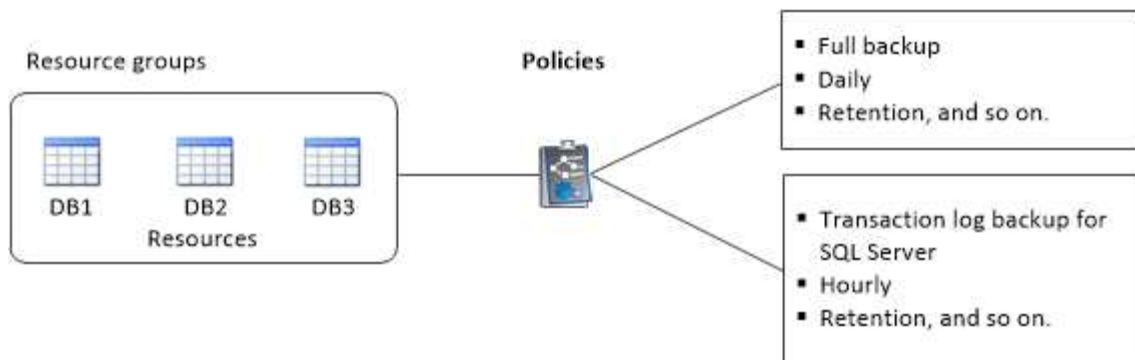
単一のリソースまたはリソース グループをオンデマンドでバックアップすることができます。また、スケジュールされたバックアップを単一リソースおよびリソース グループに対して実行することもできます。

- ポリシーは、バックアップ頻度、コピーの保持、レプリケーション、スクリプトといった、データ保護処理の特性を指定するものです。

リソース グループを作成するときに、そのグループに対して1つ以上のポリシーを選択します。単一リソースに対してオンデマンドでバックアップを実行するときにもポリシーを選択できます。

リソース グループは、保護する対象と、それを日時でいつ保護するかを定義するものと考えてください。ポリシーとは、それをどのように保護したいかを定義するものと考えてください。たとえば、すべてのデータベースまたはホストのすべてのファイルシステムをバックアップする場合、すべてのデータベースまたはホストのすべてのファイルシステムを含むリソース グループを作成します。このリソース グループに、日次ポリシーと毎時ポリシーの2つのポリシーを適用します。リソース グループを作成してポリシーを適用する際に、フル バックアップを1日1回実行するようにリソース グループを設定し、別のスケジュールでログ バックアップを1時間おきに実行するように設定します。

次の図は、データベースのリソース、リソース グループ、ポリシーの関係を示しています。



SQL Serverのデータベース、インスタンス、可用性グループのバックアップ

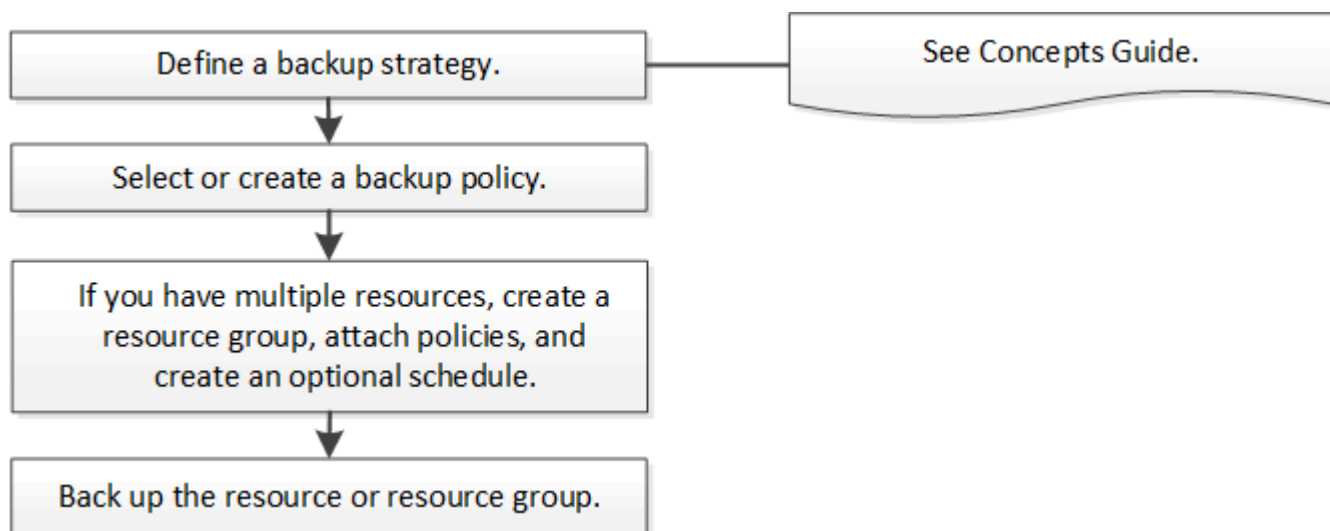
バックアップのワークフロー

SnapCenter Plug-in for Microsoft SQL Serverをインストールした環境では、SnapCenterを使用してSQL Serverリソースをバックアップすることができます。

スケジュールを設定して、複数のサーバで同時に複数のバックアップを実行することができます。

同じリソースに対してバックアップ処理とリストア処理を同時に実行することはできません。

次のワークフローは、バックアップ処理の実行順序を示しています。



NetApp以外のLUN、破損したデータベース、またはリストア中のデータベースを選択した場合、[Resources]ページの[Backup Now]、[Restore]、[Manage Backups]、[Clone]の各オプションは無効になります。

PowerShellコマンドレットを手動またはスクリプトでを使用して、バックアップ、リストア、リカバリ、検証、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、[SnapCenterコマンドレットのヘルプ](#)を使用するか、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)

SnapCenterでのデータベースのバックアップ方法

SnapCenterは、Snapshotテクノロジーを使用して、LUNまたはVMDKに格納されているSQL Serverデータベースをバックアップします。SnapCenterは、データベースのSnapshotを作成することによってバックアップを作成します。

[Resources]ページで、あるデータベースをフル データベース バックアップの対象として選択すると、同じストレージ ボリューム上の他のすべてのデータベースがSnapCenterによって自動的に選択されます。LUNまたはVMDKにデータベースが1つだけ格納されている場合は、そのデータベースを個別に選択解除したり、再度選択したりできます。LUNまたはVMDKに複数のデータベースが格納されている場合は、それらのデータベースをグループとして選択解除したり、再度選択したりする必要があります。

1つのボリューム格納されているすべてのデータベースが、Snapshotを使用して同時にバックアップされます。同時にバックアップ可能なデータベースの最大数が35で、ストレージ ボリュームに格納されているデータベースが35個よりも多い場合、データベース数を35で割った数のSnapshotが作成されます。



Snapshotごとのデータベースの最大数は、バックアップ ポリシーで設定できます。

SnapCenterで作成されるSnapshotには、ストレージ システム ボリューム全体がキャプチャされます。ただし、バックアップは、バックアップが作成されたSQLホスト サーバに対してのみ有効になります。

他のSQLホスト サーバのデータが同じボリュームに含まれている場合、それらのデータをSnapshotからリストアすることはできません。

詳細情報

"リソースの休止またはグループ化処理が失敗する"

リソースをバックアップに使用できるかどうかの確認

リソースとは、インストールしたプラグインで管理されるデータベース、アプリケーション インスタンス、可用性グループなどのコンポーネントのことです。リソースをリソース グループに追加することでデータ保護ジョブを実行できますが、その前に使用可能なリソースを特定しておく必要があります。使用可能なリソースを確認することで、プラグインのインストールが正常に完了したことの確認にもなります。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の作成、クレデンシャルの追加などのタスクを完了しておく必要があります。
- Microsoft SQLデータベースを検出するには、次のいずれかの条件を満たしている必要があります。
 - プラグイン ホストをSnapCenter Server に追加するために使用されたユーザーには、Microsoft SQL Server に対する必要な権限 (sysadmin) が必要です。
 - 上記の条件が満たされない場合は、 SnapCenter Server で、Microsoft SQL Server に対する必要な権限 (sysadmin) を持つユーザーを構成する必要があります。ユーザはMicrosoft SQL Serverインスタンス レベルで設定する必要があります。ユーザはSQLユーザまたはWindowsユーザのいずれかです。
- Windowsクラスタ内のMicrosoft SQLデータベースを検出するには、フェイルオーバー クラスタ インスタンス (FCI) のTCP/IPポートのブロックを解除する必要があります。
- データベースがVMware RDM LUNまたはVMDK上にある場合は、SnapCenter Plug-in for VMware

vSphereを導入してSnapCenterに登録する必要があります。

詳細については、"[SnapCenter Plug-in for VMware vSphereの導入](#)"

- ホストがgMSAに追加されていて、gMSAにログイン権限とシステム管理者権限がある場合は、SQLインスタンスへの接続にgMSAが使用されます。

タスク概要

詳細ページの*全体的なステータス*オプションがバックアップ不可に設定されている場合は、データベースをバックアップできません。次のいずれかに該当する場合、全体的なステータス オプションはバックアップに利用できませんに設定されます。

- データベースがNetApp LUN上にない。
- データベースが正常な状態でない。

データベースがオフライン、リストア中、リカバリの保留中、サスペクトなどの状態です。

- データベースへの十分な権限がない。

たとえば、ユーザにデータベースを表示するアクセス権しかない場合は、データベースのファイルとプロパティを特定してバックアップすることができません。



SQL Server Standard Editionに可用性グループを構成している場合、SnapCenterでバックアップできるのはプライマリ データベースのみです。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストから [データベース]、[インスタンス]、または [可用性グループ] を選択します。

をクリックし、 ホスト名とSQL Serverインスタンスを選択してリソースをフィルタリングします。そのあとにをクリックすると、フィルタ ペインが閉じます。

3. *リソースの更新*をクリックします。

新たに追加、名称変更、削除されたリソースが、SnapCenter Serverのインベントリで更新されます。



SnapCenterの外部でデータベースの名前が変更された場合は、リソースを更新する必要があります。

リソースは、リソース タイプ、ホストまたはクラスタ名、関連するリソース グループ、バックアップ タイプ、ポリシー、全体的なステータスなどの情報とともに表示されます。

- データベースがNetApp以外のストレージ上にある場合、Not available for backup *全体のステータス*列に表示されます。

NetApp以外のストレージにあるデータベースには、データ保護処理を実行できません。

- データベースがNetAppストレージ上にあり、保護されていない場合は、Not protected *全体のステータス*列に表示されます。

- データベースがNetAppストレージシステム上にあり、保護されている場合、ユーザーインターフェースには次のように表示されます。Backup not run *全体的なステータス*列にメッセージが表示されます。
- データベースがNetAppストレージシステム上にあり、保護されており、データベースのバックアップがトリガーされた場合、ユーザーインターフェースには次のように表示されます。Backup succeeded *全体的なステータス*列にメッセージが表示されます。



クレデンシャルの設定時にSQL認証を有効にすると、検出されたインスタンスやデータベースに赤い鍵マークのアイコンが表示されます。鍵マークのアイコンが表示された場合、リソースグループに追加する際にそのインスタンスまたはデータベースのクレデンシャルを指定する必要があります。

1. SnapCenter管理者が RBAC ユーザーにリソースを割り当てた後、RBAC ユーザーはログインして [リソースの更新] をクリックし、リソースの最新の 全体的なステータス を確認する必要があります。

NetAppストレージ システムへのリソースの移行

SnapCenter Plug-in for Microsoft Windowsを使用してNetAppストレージ システムをプロビジョニングしたら、SnapCenterグラフィカル ユーザ インターフェイス（GUI）またはPowerShellコマンドレットを使用して、リソースをNetAppストレージ システムに移行するか、またはあるNetApp LUNから別のNetApp LUNに移行できます。

開始する前に

- SnapCenter Serverにストレージ システムを追加しておく必要があります。
- SQL Serverリソースを更新（検出）しておく必要があります。

ウィザードの各ページのフィールドのほとんどはわかりやすいもので、説明を必要としません。以下の手順では、説明が必要な一部のフィールドを取り上げます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストから [データベース] または [インスタンス] を選択します。
3. リストからデータベースまたはインスタンスのいずれかを選択し、「移行」をクリックします。
4. [Resources] ページで、次の操作を実行します。

フィールド	操作
データベース名 (オプション)	移行対象としてインスタンスを選択した場合は、[データベース] ドロップダウン リストからそのインスタンスのデータベースを選択する必要があります。

フィールド	操作
目的地を選択	データ ファイルとログ ファイルの移行先を選択します。 データ ファイルとログ ファイルは、選択したNetAppドライブの下のDataフォルダとLogフォルダにそれぞれ移動されます。フォルダ構造にフォルダがない場合は、フォルダが作成されたうえでリソースが移行されます。
データベースファイルの詳細を表示 (オプション)	このオプションは、1つのデータベースの複数のファイルを移行する場合に選択します。  インスタンス リソースを選択した場合、このオプションは表示されません。
オプション	ソースからデータベースのコピーを削除するには、「元の場所にある移行されたデータベースのコピーを削除」を選択します。 オプション: データベースをデタッチする前に、テーブルに対して UPDATE STATISTICS を実行します。

5. [Verify]ページで、次の操作を実行します。

フィールド	操作
データベース整合性チェックオプション	移行前にデータベースの整合性を確認するには、「事前に実行」を選択します。移行後にデータベースの整合性をチェックするには、「実行後」を選択します。

フィールド	操作
DBCC CHECKDB オプション	- 整合性チェックをデータベースの物理構造に制限し、破損したページ、チェックサム障害、およびデータベースに影響する一般的なハードウェア障害を検出するには、PHYSICAL_ONLY オプションを選択します。 - すべての情報メッセージを抑制するには、NO_INFOMSGS オプションを選択します。 - オブジェクトごとに報告されたすべてのエラーを表示するには、ALL_ERRORMSGS オプションを選択します。 - 非クラスター化インデックスをチェックしない場合は、NOINDEX オプションを選択します。 SQL Serverデータベースは、Microsoft SQL ServerのDatabase Consistency Checker (DBCC) を使用して、データベース内のオブジェクトの論理的な整合性と物理的な整合性をチェックします。  このオプションを選択すると、実行時間を短縮できます。 - 内部データベース スナップショットを使用する代わりに、チェックを制限してロックを取得するには、TABLOCK オプションを選択します。

6. 概要を確認し、[完了] をクリックします。

SQL Serverデータベースのバックアップ ポリシーの作成

SnapCenterを使用してSQL Serverリソースをバックアップする前に、リソースまたはリソース グループのバックアップ ポリシーを作成することができます。また、リソースグループの作成時や単一のリソースのバックアップ時にバックアップ ポリシーを作成することも可能です。

開始する前に

- データ保護戦略を定義しておく必要があります。
- SnapCenterのインストール、ホストの追加、リソースの特定、ストレージ システム接続の作成などのタスクを実行して、データ保護の準備をしておく必要があります。
- ログ バックアップ用のホスト ログ ディレクトリを設定しておく必要があります。
- SQL Serverリソースを更新（検出）しておく必要があります。
- Snapshotをミラーまたはバックアップにレプリケートするユーザには、SnapCenter管理者がユーザに対してソースとデスティネーションの両方のボリューム用にStorage Virtual Machine (SVM) を割り当てておく必要があります。

管理者によるユーザへのリソースの割り当てについては、SnapCenterのインストール情報を参照してください。

- プリ스크립トとポストスクリプトでPowerShellスクリプトを実行する場合は、web.configファイルのusePowershellProcessforScriptsパラメータの値をtrueに設定する必要があります。

デフォルト値はfalseです。

- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、"[SnapMirrorアクティブ同期のオブジェクト数の制限](#)"。

タスク概要

- バックアップ ポリシーとは、バックアップを管理および保持する方法やリソースやリソース グループをバックアップする頻度を定めた一連のルールです。レプリケーションとスクリプトの設定を指定することもできます。ポリシーでオプションを指定しておくことで、別のリソース グループにポリシーを再利用して時間を節約することができます。

SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.ConfigファイルにあるPredefinedWindowsScriptsDirectoryキーを使用して定義します。

必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

キーの値は、API を介して Swagger から表示できます: API /4.7/configsettings

GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。

- SnapLock

- [Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで指定した保持日数以下にする必要があります。

Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、ポリシーで指定した数よりも多くのSnapshotが保持される可能性があります。

ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

ステップ1: ポリシー名を作成する

1. 左側のナビゲーション ペインで、[設定] を選択します。
2. [設定]ページで、[ポリシー]を選択します。
3. *新規*を選択します。
4. *名前*ページで、ポリシー名と詳細を入力します。

ステップ2: ポリシーオプションを構成する

1. ポリシー タイプ ページで、次の手順を実行します。
 - a. ストレージタイプを選択します。

- b. ポリシーの範囲を選択します。

フル バックアップとログ バックアップ

データベース ファイルとトランザクション ログをバックアップし、トランザクション ログを切り捨てます。

- i. *完全バックアップとログバックアップ*を選択します。
- ii. 各Snapshotにバックアップするデータベースの最大数を入力します。



同時に複数のバックアップ処理を実行する場合は、この値を増やす必要があります。

フル バックアップ

データベース ファイルをバックアップします。

- i. *完全バックアップ*を選択します。
- ii. 各Snapshotにバックアップするデータベースの最大数を入力します。デフォルト値は100です。



同時に複数のバックアップ処理を実行する場合は、この値を増やす必要があります。

ログ バックアップ

- i. トランザクション ログをバックアップします。
- ii. *ログバックアップ*を選択します。

コピーのみのバックアップ

- i. 別のバックアップ アプリケーションを使用してリソースをバックアップする場合は、[コピーのみのバックアップ]を選択します。

トランザクション ログが変更されずに保持されるため、任意のバックアップ アプリケーションでデータベースをリストアできます。通常、他の状況ではコピーのみのオプションを使用しないでください。



Microsoft SQL は、セカンダリ ストレージの 完全バックアップとログ バックアップ オプションとともに コピーのみのバックアップ オプションをサポートしていません。

ステップ3: 可用性グループの設定を構成する

1. [Availability Group Settings]セクションで、次の操作を実行します。

- a. Backup on preferred backup replica only

優先バックアップ レプリカのみをバックアップする場合は、このオプションを選択します。優先バッ

クアック レプリカは、SQL ServerのAGに対して指定されているバックアップ設定によって決まります。

- b. バックアップするレプリカを選択します。

バックアップするプライマリまたはセカンダリのAGレプリカを選択します。

- c. バックアップ優先度（最小および最大のバックアップ優先度）を選択します

バックアップするAGレプリカを決めるための、バックアップの最小優先順位と最大優先順位を指定します。たとえば、最小優先順位を10、最大優先順位を50に設定すると、優先順位が10より高く50より低いすべてのAGレプリカがバックアップ用とみなされます。

デフォルトでは、最小優先順位は1、最大優先順位は100です。



クラスタ構成では、ポリシーで設定された保持設定に従って、バックアップがクラスタの各ノードに保持されます。AGの所有者ノードが変更された場合、保持設定に従ってバックアップが作成され、以前の所有者ノードのバックアップが保持されます。AGの保持設定はノード レベルでのみ適用されます。

ステップ4: スナップショットとレプリケーションの設定を構成する

1. スナップショットとレプリケーション ページで、次の手順を実行します。

- a. オンデマンド、時間別、日次、週次、または*月次*を選択してスケジュール タイプを指定します。

ポリシーに対して選択できるスケジュール タイプは1つだけです。



リソース グループを作成する際に、バックアップ処理のスケジュール（開始日、終了日、および頻度）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソース グループを作成できますが、各ポリシーに異なるバックアップ スケジュールを割り当てることもできます。



午前 2 時にスケジュールを設定した場合、夏時間 (DST) 中はスケジュールは実行されません。

ステップ5: 最新の保持設定を構成する

1. 「最新の保持設定」セクションで、バックアップ タイプ ページで選択したバックアップ タイプに応じて、次のアクションの 1 つ以上を実行します。

特定のコピー数

特定の数のSnapshotのみを保持します。

1. 過去 <数値> 日間のログ バックアップを保持する オプションを選択し、保持する日数を指定します。この上限に近づいた場合は、古いコピーを削除できます。

特定の日数

バックアップ コピーを特定の日数だけ保持します。

1. [過去 <数値> 日間の完全バックアップに適用可能なログ バックアップを保持する] オプションを選択し、ログ バックアップ コピーを保持する日数を指定します。

ステップ6: スナップショットの設定を構成する

1. 完全バックアップの保持設定では、次の操作を実行します。

- a. 保存するスナップショットの合計数を指定します

- i. 保持するスナップショットの数を指定するには、[保持するコピー数] を選択します。
- ii. Snapshotの数が指定した数を超えると、古いものから順にSnapshotが削除されます。



デフォルトでは、保持数の値は2に設定されています。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。



最大保持値は 1018 です。保持期間が基盤となるNetApp ONTAPバージョンでサポートされている値よりも高い値に設定されている場合、バックアップは失敗します。

2. スナップショットを保存する期間

- a. スナップショットを削除する前に保持する日数を指定する場合は、「コピーを保持する期間」を選択します。

3. スナップショット コピーのロック期間 を選択し、期間を日数、月数、または年数で指定します。

SnapLock保持期間は100年未満にする必要があります。

4. ポリシーラベルを選択します。



リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしなくても実行できます。

ステップ7: セカンダリレプリケーションオプションを構成する

1. [セカンダリ レプリケーション オプションの選択] セクションで、次のセカンダリ レプリケーション オプションの 1 つまたは両方を選択します。

SnapMirror を更新

ローカル Snapshot コピーの作成後に SnapMirror を更新

1. 別のボリュームにバックアップ セットのミラー コピーを作成する場合 (SnapMirror) は、このオプションを選択します。

このオプションは、SnapMirrorアクティブ同期に対して有効にする必要があります。

セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。

見る"[[Topology](#)ページでのSQL Serverのバックアップとクローンの表示]"。

SnapVault を更新

Snapshotコピーの作成後にSnapVaultを更新します。

1. ディスクツーディスクのバックアップ レプリケーションを実行する場合は、このオプションを選択します。

セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。

SnapLock がSnapLock Vault と呼ばれるONTAPのセカンダリにのみ設定されている場合、[トポロジ] ページの [更新] ボタンをクリックすると、ONTAPから取得されたセカンダリのロック期間が更新されます。

SnapLock Vaultの詳細については、"[バックアップ デスティネーションのSnapshotコピーのWORM 状態へのコミット](#)"

見る"[[Topology](#)ページでのSQL Serverのバックアップとクローンの表示]"。

エラー時の再試行回数

1. レプリケーションの最大試行回数を入力します。この回数を超えると処理が停止します。

ステップ8: スクリプト設定を構成する

1. [Script]ページで、バックアップ処理の前またはあとに実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

たとえば、SNMPトラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。



プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。



セカンダリ ストレージがSnapshotの最大数に達しないように、ONTAPでSnapMirrorの保持ポリシーを設定する必要があります。

ステップ9: 検証設定を構成する

[Verification]ページで、次の手順を実行します。

1. [Run verification for following backup schedules]セクションで、実行頻度を選択します。
2. [Database consistency check options]セクションで、次の操作を実行します。
 - a. Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)
 - i. 整合性チェックをデータベースの物理構造に制限し、破損したページ、チェックサム障害、およびデータベースに影響する一般的なハードウェア障害を検出するには、[整合性構造をデータベースの物理構造に制限する (PHYSICAL_ONLY)] を選択します。
 - b. Suppress all information messages (NO_INFOMSGS)
 - i. すべての情報メッセージを抑制するには、[すべての情報メッセージを抑制 (NO_INFOMSGS)] を選択します。このオプションはデフォルトで選択されています。
 - c. Display all reported error messages per object (ALL_ERRORMSGs)
 - i. オブジェクトごとに報告されたすべてのエラーを表示するには、オブジェクトごとに報告されたすべてのエラー メッセージを表示する (**ALL_ERRORMSGs**) を選択します。
 - d. Do not check nonclustered indexes (NOINDEX)
 - i. 非クラスター化インデックスをチェックしない場合は、[非クラスター化インデックスをチェックしない (NOINDEX)] を選択します。SQL Serverデータベースは、Microsoft SQL Server のDatabase Consistency Checker (DBCC) を使用して、データベース内のオブジェクトの論理的な整合性と物理的な整合性をチェックします。
 - e. 内部データベーススナップショット (TABLOCK) を使用する代わりに、チェックを制限してロックを取得します。
 - i. 内部データベース スナップショットを使用する代わりにチェックを制限し、ロックを取得するには、[内部データベース スナップショット コピーを使用する代わりにチェックを制限し、ロックを取得する (**TABLOCK**)] を選択します。
3. ログ バックアップ セクションで、完了時にログ バックアップを検証する を選択して、完了時にログ バックアップを検証します。
4. *検証スクリプト設定*セクションで、検証操作の前または後に実行するプレスクリプトまたはポストスクリプトのパスと引数を入力します。



プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

ステップ10: 概要を確認する

1. 概要を確認し、[完了] を選択します。

SQL Serverに対するリソース グループの作成とポリシーの適用

リソース グループはコンテナであり、一緒にバックアップして保護するリソースをここに追加します。リソース グループを使用することで、特定のアプリケーションに関連するすべてのデータを同時にバックアップできます。リソース グループはいずれのデータ保護ジョブにも必要になります。リソース グループに1つ以上のポリシーを適用して、

実行するデータ保護ジョブのタイプを定義することも必要です。

リソースを個別に保護する場合、新しいリソース グループを作成する必要はありません。保護されたリソースでバックアップを作成することができます。

タスク概要

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期を使用するリソースを含む既存のリソース グループにSnapMirrorアクティブ同期を使用しない新しいデータベースを追加することはできません。
- SnapMirrorアクティブ同期のフェイルオーバー モードである既存のリソース グループに新しいデータベースを追加することはできません。リソースを追加できるのは、通常の状態またはフェイルバック状態のリソース グループのみです。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] を選択します。



SnapCenterに最近リソースを追加した場合は、[リソースの更新] をクリックして、新しく追加されたリソースを表示します。

3. *新しいリソース グループ*をクリックします。
4. [Name]ページで、次の操作を実行します。

フィールド	操作
Name	リソース グループ名を入力します。 リソース グループ名は250文字以内で指定する必要があります。
Tags	リソース グループを検索しやすくするために、ラベルを入力します。たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。
Use custom name format for Snapshot copy	オプション: カスタム スナップショットの名前と形式を入力します。たとえば、customtext_resourcegroup_policy_hostname やresourcegroup_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

5. [Resources]ページで、次の手順を実行します。
 - a. ホスト名、リソース タイプ、およびSQL Serverインスタンスをドロップダウン リストから選択し

て、リソースのリストをフィルタリングします。



最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources]のリストには表示されません。

- b. 利用可能なリソース セクションから選択したリソース セクションにリソースを移動するには、次のいずれかの手順を実行します。

- 同じボリューム上のすべてのリソースを「選択したリソース」セクションに移動するには、「同じストレージ ボリューム上のすべてのリソースを自動選択」を選択します。
- *利用可能なリソース*セクションからリソースを選択し、右矢印をクリックして*選択したリソース*セクションに移動します。

6. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます 。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. 選択したポリシーのスケジュールを構成するセクションで、*をクリックします。  * スケジュールを構成するポリシーの [スケジュールの構成] 列で、
- c. [ポリシー *policy_name* のスケジュールの追加] ダイアログ ボックスで、開始日、有効期限、頻度を指定してスケジュールを構成し、[OK] をクリックします。

この操作は、ポリシーに指定されている頻度ごとに実行する必要があります。構成されたスケジュールは、[選択したポリシーのスケジュールを構成する] セクションの [適用されたスケジュール] 列に表示されます。

- d. [Microsoft SQL Server scheduler]を選択します。

スケジューリング ポリシーに関連付けるスケジューラ インスタンスも選択する必要があります。

[Microsoft SQL Server scheduler]を選択しなかった場合は、デフォルトで[Microsoft Windows scheduler]に設定されます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。WindowsスケジューラまたはSQL Serverエージェントで作成されたスケジュールを変更したり、バックアップ ジョブの名前を変更したりしないでください。

7. [Verification]ページで、次の手順を実行します。

- a. *検証サーバー*ドロップダウンリストから検証サーバーを選択します。

このリストには、SnapCenterで追加されたすべてのSQL Serverが含まれます。検証サーバ（ローカルホストまたはリモート ホスト）は複数選択できます。



検証サーバのバージョンは、プライマリ データベースをホストしているSQL Serverのバージョンおよびエディションと一致している必要があります。

- a. ロケータのロード をクリックして、 SnapMirrorおよびSnapVaultボリュームをロードし、セカンダリストレージで検証を実行します。
- b. 検証スケジュールを設定するポリシーを選択し、*をクリックします。  *。
- c. [Add Verification Schedules policy_name]ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択します。

- d. [OK]をクリックします。

設定したスケジュールが[Applied Schedules]列にリストされます。をクリックすると確認して編集で

きます  またはクリックして削除 *  *。

8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

9. 概要を確認し、[完了] をクリックします。

関連情報

"SQL Serverデータベースのバックアップ ポリシーの作成"

リソース グループを作成し、 **ASA r2** システム上の **Microsoft SQL Server** リソースの二次保護を有効にします。

ASA r2 システム上にあるリソースを追加するには、リソース グループを作成する必要があります。リソース グループの作成時にセカンダリ保護をプロビジョニングすることもできます。

開始する前に

- ONTAP 9.x リソースとASA r2 リソースの両方を同じリソース グループに追加していないことを確認する必要があります。
- ONTAP 9.x リソースとASA r2 リソースの両方を含むデータベースが存在しないことを確認する必要があります。

タスク概要

- 二次保護は、ログインしたユーザーに **SecondaryProtection** 機能が有効になっているロールが割り当てられている場合にのみ使用できます。

- セカンダリ保護を有効にすると、プライマリおよびセカンダリ整合性グループの作成中にリソース グループはメンテナンス モードになります。プライマリおよびセカンダリのコンシステンシー グループが作成されると、リソース グループのメンテナンス モードが解除されます。
- SnapCenter はクローン リソースの二次保護をサポートしていません。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。
 - a. [Name] フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag] フィールドに1つ以上のラベルを入力します。

たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

- c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- d. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。



必要に応じて、プレフィックスを含め、アプリケーションで設定されたのと同じ宛先を使用する必要があります。

4. [リソース] ページで、[ホスト] ドロップダウン リストからデータベース ホスト名を選択します。



[Available Resources] セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources] のリストには表示されません。

5. [使用可能なリソース] セクションからASA r2 リソースを選択し、[選択したリソース] セクションに移動します。
6. アプリケーション設定ページで、バックアップ オプションを選択します。
7. [Policies] ページで、次の手順を実行します。
 - a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックし  でポリシーを作成することもできます。

[Configure schedules for selected policies] セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。
- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 選択したポリシーに対して二次保護が有効になっている場合は、「二次保護」ページが表示されるので、次の手順を実行する必要があります。

- a. レプリケーション ポリシーのタイプを選択します。



同期レプリケーション ポリシーはサポートされていません。

- b. 使用する整合性グループのサフィックスを指定します。
- c. [宛先クラスタ] および [宛先 SVM] ドロップダウンから、使用するピア クラスタと SVM を選択します。



クラスタと SVM のピアリングはSnapCenterではサポートされていません。クラスタと SVM のピアリングを実行するには、System Manager またはONTAP CLI を使用する必要があります。



リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは [セカンダリ保護リソース] セクションに表示されます。

1. [Verification]ページで、次の手順を実行します。

- a. ロケーターのロード をクリックして、 SnapMirrorまたはSnapVaultボリュームをロードし、セカンダリストレージで検証を実行します。
- b. クリック  ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で をクリックします。
- c. [Add Verification Schedules *policy_name*]ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

- d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証] を選択します。

e. [OK]をクリックします。

設定した検証スケジュールが、[Applied Schedules]列にリストされます。

2. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

3. 概要を確認し、[完了] をクリックします。

SQLリソースのバックアップの要件

SQLリソースをバックアップする前に、以下の要件を満たしていることを確認する必要があります。

- 他社ストレージ システムからNetAppストレージ システムにリソースを移行しておく必要があります。
- バックアップ ポリシーを作成しておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。
- Active Directory (AD) ユーザが開始したバックアップ処理は、そのADユーザまたはグループにSQLインスタンスのクレデンシャルが割り当てられていないと失敗します。設定 > ユーザー アクセス ページから、SQL インスタンス資格情報を AD ユーザーまたはグループに割り当てる必要があります。
- ポリシーを適用したリソース グループを作成しておく必要があります。
- リソース グループにホストが異なる複数のデータベースが含まれている場合、ネットワークの問題が原因で、一部のホストでのバックアップ処理のトリガーが遅れることがあります。PowerShellのSet-SmConfigSettingsコマンドレットを使用して、web.configのFMaxRetryForUninitializedHostsの値を設定する必要があります。

PowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成

PowerShellコマンドレットを使用してデータ保護処理を実行するには、Storage Virtual Machine (SVM) 接続とクレデンシャルを作成しておく必要があります。

開始する前に

- PowerShellコマンドレットを実行できるようにPowerShell環境を準備しておく必要があります。
- ストレージ接続を作成するには、Infrastructure Adminロールの権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

ストレージ システム接続の追加中は、ホスト プラグインのインストールが進行中であってはなりません。ホスト キャッシュが更新されず、SnapCenter GUI にデータベースのステータスが「バックアップに

使用できません」または「NetAppストレージ上にありません」と表示される可能性があるためです。

- ストレージ システムの名前は一意である必要があります。

SnapCenterでは、別々のクラスタに属している場合でも、複数のストレージ システムに同じ名前を付けることはサポートされません。SnapCenterでサポートする各ストレージ システムには、一意な名前と管理LIFの一意なIPアドレスが必要です。

手順

1. Open-SmConnectionコマンドレットを使用して、PowerShell Core接続セッションを開始します。

PowerShellセッションを開く例を次に示します。

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

2. Add-SmStorageConnectionコマンドレットを使用して、ストレージ システムへの新しい接続を作成します。

新しいストレージ システム接続を作成する例を次に示します。

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Add-SmCredentialコマンドレットを使用して、新しいクレデンシャルを作成します。

Windowsクレデンシャルを使用してFinanceAdminという名前の新しいクレデンシャルを作成する例を次に示します。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

SQLリソースのバックアップ

どのリソース グループにもまだ含まれていないリソースは、[Resources]ページからバックアップすることができます。

タスク概要

- バックアップ操作を最適化するには、DNS サーバーに Windows クラスター名と IP アドレスの逆引き参照レコードを作成する必要があります。
- Windowsクレデンシャル認証については、プラグインのインストール前にクレデンシャルを設定する必要があります。

- SQL Serverインスタンス認証については、プラグインのインストール後にクレデンシャルを追加する必要があります。
- gMSA 認証の場合、gMSA を有効にして使用するには、ホストの追加 または ホストの変更 ページでSnapCenterにホストを登録するときに gMSA を設定する必要があります。
- ホストがgMSAに追加されていて、gMSAにログイン権限とシステム管理者権限がある場合は、gMSAはSQLインスタンスに接続できます。
 - SnapCenterは、SQLインスタンスの認証が設定されているかどうかを検証します。認証が設定されている場合、このクレデンシャルを使用してSQLインスタンスにアクセスできます。
 - 認証が設定されていない場合は、gMSAを使用してSQLプラグインが現在動作しているかどうかを確認します。プラグインが動作している場合は、SQLインスタンスへの接続を確立するために使用されます。
 - SQLインスタンスの認証が設定されておらず、プラグインも動作していない場合、SQLインスタンスにはWindowsクレデンシャルの認証を介してアクセスできます。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストから [データベース]、[インスタンス]、または [可用性グループ] を選択します。

- a. バックアップするデータベース、インスタンス、または可用性グループを選択します。

インスタンスをバックアップする場合、そのインスタンスの前のバックアップ ステータスやタイムスタンプに関する情報はリソース ページに表示されません。

トポロジ ビューでは、バックアップ ステータス、タイムスタンプ、またはバックアップが、インスタンスのものかデータベースのものを区別できません。

3. [リソース] ページで、[スナップショット コピーのカスタム名形式] チェック ボックスをオンにし、スナップショット名に使用するカスタム名形式を入力します。

たとえば、`customtext_policy_hostname`や`resource_hostname`などです。デフォルトでは、Snapshot の名前の後ろにタイムスタンプが付加されます。

4. [Policies] ページで、次の作業を実行します。

- a. [Policies] セクションで、ドロップダウン リストから1つ以上のポリシーを選択します。

を選択してポリシーを作成できます  ポリシー ウィザードを起動します。

*選択したポリシーのスケジュールを構成する*セクションに、選択したポリシーがリストされます。

- b.  を選択  スケジュールを構成するポリシーの [スケジュールの構成] 列で、

- c. ポリシーのスケジュールを追加 `policy\_name` ダイアログボックスでスケジュールを構成し、[OK] を選択します。

ここ `policy\_name` 選択したポリシーの名前です。

構成されたスケジュールは、「適用されたスケジュール」列にリストされます。

- a. **Microsoft SQL Server** スケジューラを使用する を選択し、スケジュール ポリシーに関連付けられている スケジューラ インスタンス ドロップダウン リストからスケジューラ インスタンスを選択します。

5. [Verification] ページで、次の手順を実行します。

- a. *検証サーバー*ドロップダウンリストから検証サーバーを選択します。

検証サーバ（ローカル ホストまたはリモート ホスト）は複数選択できます。



検証サーバのバージョンは、プライマリ データベースをホストしているSQL Serverのエディションのバージョン以降である必要があります。

- a. セカンダリ ストレージ システム上のバックアップを検証するには、セカンダリ ロケーターをロードしてセカンダリ上のバックアップを検証する を選択します。
- b. 検証スケジュールを設定するポリシーを選択し、*を選択します。  *。
- c. 「検証スケジュールの追加 *policy_name*」 ダイアログ ボックスで、次のアクションを実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択します。



検証サーバーにストレージ接続がない場合、検証操作は「ディスクのマウントに失敗しました」というエラーで失敗します。

- d. 「OK」を選択します。

設定したスケジュールが[Applied Schedules]列にリストされます。

6. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソース グループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtptServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

7. 概要を確認し、[完了] を選択します。

データベース トポロジのページが表示されます。

8. *今すぐバックアップ*を選択します。

9. [Backup]ページで次の手順を実行します。

- a. リソースに複数のポリシーを適用している場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. バックアップを検証するには、「バックアップ後に検証」を選択します。
- c. *バックアップ*を選択します。



WindowsスケジューラやSQL Serverエージェントで作成されたバックアップ ジョブの名前は変更しないでください。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

暗黙的リソース グループが作成されます。これを表示するには、[User Access]ページで対応するユーザまたはグループを選択します。暗黙的なリソース グループ タイプは「Resource」です。

10. モニター > ジョブ を選択して、操作の進行状況を監視します。

終了後の操作

- MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

"MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"

- VMDK上のアプリケーション データをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープ サイズが不足していると、バックアップが失敗することがあります。Javaヒープ サイズを増やすには、スクリプト ファイル/opt/netapp/init_scripts/scvserviceを探します。その脚本では、do_start method`コマンドは、 SnapCenter VMware プラグイン サービスを開始します。このコマンドを次のように更新します。 `Java -jar -Xmx8192M -Xms4096M。

関連情報

"SQL Serverデータベースのバックアップ ポリシーの作成"

"TCP_TIMEOUTでの遅延のためにMySQL接続エラーが発生して、バックアップ処理が失敗する"

"Windowsスケジューラのエラーでバックアップが失敗する"

"リソースの休止またはグループ化処理が失敗する"

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmPolicyコマンドレットを使用して、バックアップ ポリシーを作成します。

この例では、SQLのバックアップ タイプ「FullBackup」を指定して新しいバックアップ ポリシーを作成しています。

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

この例では、Windowsファイルシステムのバックアップ タイプ「CrashConsistent」を指定して新しいバックアップ ポリシーを作成しています。

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Get-SmResourcesコマンドレットを使用してホスト リソースを検出します。

この例では、指定したホスト上でMicrosoft SQLプラグインのリソースを検出しています。

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

この例では、指定したホスト上でWindowsファイルシステムのリソースを検出しています。

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Add-SmResourceGroupコマンドレットを使用して、SnapCenterに新しいリソース グループを追加します。

この例では、ポリシーとリソースを指定して新しいSQLデータベース バックアップ リソース グループを作成しています。

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

この例では、ポリシーとリソースを指定して新しいWindowsファイルシステム バックアップ リソース グループを作成しています。

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. New-SmBackupコマンドレットを使用して、新しいバックアップ ジョブを開始します。

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy FinancePolicy
```

6. Get-SmBackupReportコマンドレットを使用して、バックアップ ジョブのステータスを表示します。

この例では、指定した日に実行されたすべてのジョブの概要レポートを表示しています。

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

SQL Serverリソース グループのバックアップ

リソース グループは、[Resources]ページからオンデマンドでバックアップできます。リソース グループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが行われます。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。

リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、 をクリックして、タグを選択します。次に選択できます  フィルター パネルを閉じます。

3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] を選択します。
4. [Backup]ページで次の手順を実行します。

- a. リソース グループに複数のポリシーを関連付けている場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. バックアップ後、「検証」を選択してオンデマンド バックアップを検証します。

ポリシーの **Verify** オプションは、スケジュールされたジョブにのみ適用されます。

- c. *バックアップ*を選択します。

5. モニター > ジョブ を選択して、操作の進行状況を監視します。

関連情報

"SQL Serverデータベースのバックアップ ポリシーの作成"

"SQL Serverに対するリソース グループの作成とポリシーの適用"

"TCP_TIMEOUTでの遅延のためにMySQL接続エラーが発生して、バックアップ処理が失敗する"

"Windowsスケジューラのエラーでバックアップが失敗する"

SnapCenterの[Jobs]ページでのSQLリソースのバックアップ処理の監視

SnapCenterの[Jobs]ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*ジョブ*をクリックします。
3. [Jobs]ページで、次の手順を実行します。
 - a. をクリックして、 リストの内容をバックアップ処理だけに絞り込みます。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*バックアップ*を選択します。
 - d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. バックアップ ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスは  ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[Activity]ペインでのSQLリソースのデータ保護処理の監視

[Activity]ペインには、最後に実行された5つの処理が表示されます。また[Activity]ペインには、処理が開始された日次と処理のステータスが表示されます。

[Activity]ペインには、バックアップ、リストア、クローニング、スケジュールされたバックアップの各処理に関する情報が表示されます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. クリック  アクティビティ ペインで、最新の 5 つの操作を表示します。

いずれかの操作をクリックすると、*ジョブの詳細*ページに操作の詳細が表示されます。

SnapCenter Plug-in for Microsoft SQL Serverのバックアップ処理のキャンセル

実行中、キューに登録済み、または応答なしのバックアップ処理はキャンセルできません。バックアップ処理をキャンセルすると、SnapCenter Serverにより処理が停止されます。作成されたバックアップがSnapCenter Serverに登録されていない場合、ストレージからすべてのSnapshotが削除されます。バックアップがすでにSnapCenter Serverに登録されている場合、キャンセルがトリガーされても、すでに作成されているSnapshotはロールバックされません。

開始する前に

- リストア処理をキャンセルするには、SnapCenter管理者またはジョブ所有者としてログインする必要があります。
- キャンセルできるのは、キューに登録済みまたは実行中のログ バックアップ処理またはフル バックアップ処理だけです。
- 検証の開始後は、処理をキャンセルできません。

検証前に処理をキャンセルすると、処理はキャンセルされ、検証処理は実行されません。

- バックアップ処理は、[Monitor]ページまたは[Activity]ペインでキャンセルできます。
- SnapCenter GUIに加え、PowerShellコマンドレットを使用して処理をキャンセルすることもできます。
- キャンセルできない操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたバックアップ操作をキャンセルできます。

手順

次のいずれかを実行します。

方法	アクション
[Monitor]ページ	1. 左側のナビゲーション ペインで、モニター > ジョブ を選択します。 2. ジョブを選択し、[ジョブのキャンセル]を選択します。
[Activity]ペイン	1. バックアップジョブを開始した後、 アクティビティ ペインで、最新の 5 つの操作を表示します。 2. 処理を選択します。 3. ジョブの詳細ページで、*ジョブのキャンセル*を選択します。

結果

処理がキャンセルされ、リソースは処理前の状態に戻ります。キャンセルした操作がキャンセル中または実行中の状態で応答しない場合は、`Cancel-SmJob -JobID <int> -Force`バックアップ操作を強制的に停止するコマンドレット。

[Topology]ページでのSQL Serverのバックアップとクローンの表示

リソースのバックアップまたはクローニングを準備する際に、プライマリ ストレージとセカンダリ ストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。

タスク概要

[Topology]ページでは、選択したリソースまたはリソース グループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を参照し、対象を選択してデータ保護処理を実行できます。

コピーの管理 ビューで次のアイコンを確認して、バックアップとクローンがプライマリ ストレージまたはセカンダリ ストレージ (ミラー コピーまたは Vault コピー) で使用可能かどうかを確認できます。

- 
 プライマリ ストレージで使用可能なバックアップとクローンの数を表示します。
- 
 SnapMirrorテクノロジーを使用してセカンダリ ストレージにミラーリングされているバックアップとクローンの数を表示します。
- 
 SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップとクローンの数を表示します。
 - 表示されるバックアップの数には、セカンダリ ストレージから削除されたバックアップも含まれません。

たとえば、バックアップを4個保持するポリシーを使用してバックアップを6個作成した場合、バックアップの数は6個と表示されます。



mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップの数にはバージョンに依存しないバックアップは含まれません。

SnapMirrorアクティブ同期 (当初はSnapMirror Business Continuity [SM-BC] としてリリース) としてセカンダリ関係がある場合は、次の追加アイコンが表示されます。

-  レプリカサイトが稼働しています。
-  レプリカサイトはダウンしています。
-  セカンダリ ミラーまたはボールド関係が再確立されていません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストからリソースまたはリソース グループを選択します。
3. リソースの詳細ビューまたはリソース グループの詳細ビューで、リソースを選択します。

選択したリソースがクローニングされたデータベースである場合は、クローニングされたデータベースが保護され、クローンのソースが[Topology]ページに表示されます。クローン作成に使用されたバックアップを表示するには、「詳細」をクリックします。

リソースが保護されている場合は、選択したリソースの[Topology]ページが表示されます。

4. [Summary Card]で、プライマリ ストレージとセカンダリ ストレージ上にあるバックアップとクローンの数の概要を確認します。

*概要カード*セクションには、バックアップとクローンの合計数が表示されます。

更新 ボタンをクリックすると、ストレージのクエリが開始され、正確な数が表示されます。

SnapLock対応バックアップが取得された場合、[更新] ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでも、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

アプリケーション リソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限はONTAPから取得されます。

SnapMirrorアクティブ同期の場合、[更新] ボタンをクリックすると、プライマリ サイトとレプリカ サイトの両方に対してONTAPを照会してSnapCenterバックアップ インベントリが更新されます。週次スケジュールでも、SnapMirrorアクティブ同期関係を含むすべてのデータベースに対してこの処理が実行されます。

- SnapMirrorアクティブ同期とONTAP（バージョン9.14.1のみ）では、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップの関係については、フェイルオーバー

後に手動で設定する必要があります。ONTAP 9.15.1以降は、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップが、自動的に設定されます。

- 。フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。バックアップが作成された後にのみ、「更新」をクリックできます。

5. コピーの管理 ビューで、プライマリ ストレージまたはセカンダリ ストレージから バックアップ または クローン をクリックして、バックアップまたはクローンの詳細を表示します。

バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、名前変更、削除の各処理を実行します。



セカンダリ ストレージ上のバックアップは、名前変更または削除できません。

7. テーブルからクローンを選択し、「クローン分割」をクリックします。
8. クローンを削除する場合は、表でクローンを選択し、 をクリックします。

PowerShellコマンドレットを使用したセカンダリ バックアップ数のクリーンアップ

Remove-SmBackupコマンドレットを使用して、Snapshotがないセカンダリ バックアップのバックアップ数をクリーンアップできます。コピーの管理トポロジに表示されるスナップショットの合計がセカンダリ ストレージのスナップショット保持設定と一致しない場合に、このコマンドレットを使用することをお勧めします。

PowerShellコマンドレットを実行できるように環境を準備しておく必要があります。

コマンドレットで使用するパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146/
```

2. -CleanupSecondaryBackupsパラメータを使用してセカンダリ バックアップ数をクリーンアップします。

この例では、Snapshotがないセカンダリ バックアップのバックアップ数をクリーンアップしています。

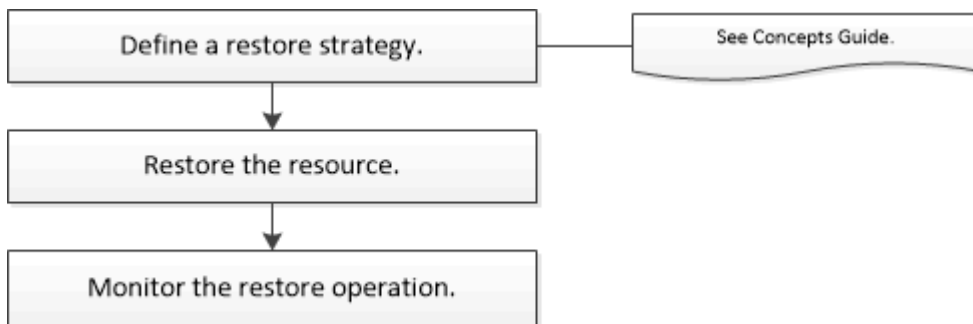
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

SQL Serverリソースのリストア

リストアのワークフロー

SnapCenterを使用して1つ以上のバックアップからアクティブ ファイルシステムにデータをリストアし、データベースをリカバリすることで、SQL Serverデータベースをリストアできます。可用性グループ内のデータベースをリストアし、リストアしたデータベースを可用性グループに追加することもできます。SQL Serverデータベースをリストアする前に、いくつかの準備作業を実行する必要があります。

次のワークフローは、データベース リストア処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、リカバリ、検証、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、[SnapCenterコマンドレットのヘルプ](#)を使用するか、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)

詳細情報

["セカンダリ ストレージからSQL Serverデータベースのリストア"](#)

["PowerShellコマンドレットを使用したリソースのリストアおよびリカバリ"](#)

["SnapCenter, Restore operation might fail on Windows 2008 R2"](#)

データベースをリストアする際の要件

SnapCenter Plug-in for Microsoft SQL ServerのバックアップからSQL Serverデータベースをリストアする前に、以下の要件を満たしていることを確認する必要があります。

- ターゲットSQL Serverインスタンスがオンラインで、稼働している必要があります。

これは、ユーザ データベースのリストア処理とシステム データベースのリストア処理の両方に当てはまります。

- リモート管理サーバまたはリモート検証サーバ上でスケジュールされているジョブも含め、リストアするSQL Serverデータに対して実行予定のSnapCenter処理をすべて無効にしておく必要があります。
- システム データベースが機能していない場合は、最初にSQL Serverユーティリティを使用してシステムデータベースを再構築しておく必要があります。
- プラグインをインストールするときに、可用性グループ（AG）のバックアップをリストアする権限を他

のロールに付与します。

次のいずれかの条件に該当する場合、AGのリストアが失敗します。

- RBACユーザがプラグインをインストールし、管理者がAGバックアップをリストアしようとした場合
- 管理者がプラグインをインストールし、RBACユーザがAGバックアップをリストアしようとした場合
- カスタム ログ ディレクトリのバックアップを代替ホストにリストアする場合は、SnapCenter Serverとプラグイン ホストに同じバージョンのSnapCenterがインストールされている必要があります。
- Microsoftの更新プログラムKB2887595をインストールしておく必要があります。KB2887595の詳細については、Microsoftのサポート サイトを参照してください。

["Microsoft サポート記事 2887595: Windows RT 8.1、Windows 8.1、および Windows Server 2012 R2 更新プログラムのロールアップ: 2013 年 11 月"](#)

- リソース グループまたはデータベースをバックアップしておく必要があります。
- Snapshotをミラーまたはバックアップにレプリケートするユーザには、SnapCenter管理者がユーザに対してソースとデスティネーションの両方のボリューム用にStorage Virtual Machine (SVM) を割り当てておく必要があります。

管理者によるユーザへのリソースの割り当てについては、SnapCenterのインストール情報を参照してください。

- データベースをリストアする前に、すべてのバックアップ ジョブとクローン ジョブを停止しておく必要があります。
- データベースのサイズがテラバイト (TB) 単位の場合、リストア処理がタイムアウトになることがあります。

次のコマンドを実行して、SnapCenter Server の RESTTimeout パラメータの値を 20000000 ミリ秒に増やす必要があります: `Set-SmConfigSettings -Agent -configSettings @"{\"RESTTimeout\" = \"20000000\"}`。タイムアウト値は、データベースのサイズに応じて変更できます。設定可能な最大値は、86,400,000ミリ秒です。

データベースがオンライン状態のときにリストアする場合は、[Restore]ページでオンライン リストア オプションを有効にする必要があります。

SQL Serverデータベースのバックライトのリストア

SnapCenterを使用して、バックアップされたSQL Serverデータベースをリストアすることができます。データベース リストアは段階的に実施され、すべてのデータとログ ページが指定したSQL Serverバックアップから指定したデータベースにコピーされます。

タスク概要

- バックアップされたSQL Serverデータベースを、バックアップが作成されたホスト上の別のSQL Server インスタンスにリストアすることができます。

本番バージョンを上書きしてしまわないように、SnapCenterではバックアップされたSQL Serverデータベースを別のパスにリストアすることができます。

- SnapCenterでは、WindowsクラスタのデータベースをSQL Serverクラスタ グループをオフラインにする

ことなくリストアできます。

- リストア処理中に、リソースを所有するノードがダウンするなどのクラスタ障害（クラスタ グループの移動処理）が発生した場合は、SQL Serverインスタンスに再接続してからリストア処理を再開する必要があります。
- ユーザまたはSQL Server Agentジョブがアクセス中のデータベースはリストアできません。
- システム データベースは別のパスにリストアできません。
- SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.ConfigファイルにあるPredefinedWindowsScriptsDirectoryキーを使用して定義します。

必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

キーの値は、API を介して Swagger から表示できます: [API /4.7/configsettings](#)

GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。

- [Restore]ウィザードの各ページのフィールドのほとんどはわかりやすいもので、説明を必要としません。以下の手順では、説明が必要なフィールドを取り上げます。
- SnapMirrorアクティブ同期でリストア処理を実行するには、プライマリの場所からバックアップを選択する必要があります。
- SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotのロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

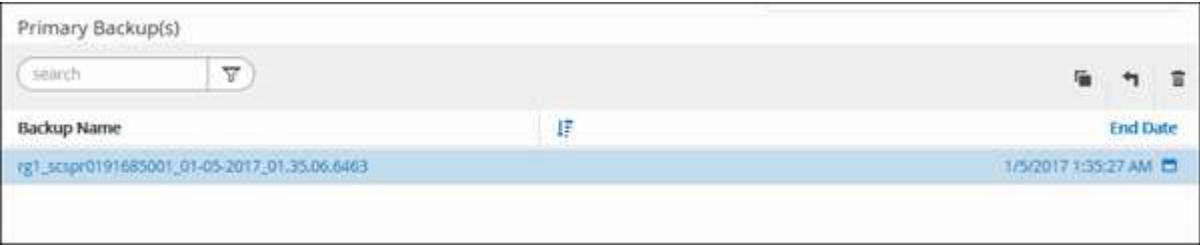
SnapCenter UI

手順

- 1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
- 2. [リソース] ページで、[表示] リストから [データベース] または [リソース グループ] を選択します。
- 3. リストからデータベースまたはリソース グループを選択します。

トポロジ ページが表示されます。

- 4. [コピーの管理] ビューで、ストレージ システムから [バックアップ] を選択します。
- 5. 表からバックアップを選択し、 アイコン。



- 6. [Restore Scope] ページで、次のいずれかのオプションを選択します。

オプション	説明
バックアップが作成されたホストにデータベースをリストア	バックアップが作成されたのと同じ SQL Server にデータベースをリストアする場合は、このオプションを選択します。
別のホストにデータベースをリストア	バックアップが作成されたホストまたは別のホスト内にある別の SQL Server にデータベースをリストアする場合は、このオプションを選択します。 ホスト名を選択し、データベース名を入力し（オプション）、インスタンスを選択し、リストア パスを指定します。  代替パスに指定するファイル拡張子は、元のデータベース ファイルのファイル拡張子と同じにする必要があります。 「復元スコープ」ページに「データベースを別のホストに復元する」オプションが表示されない場合は、ブラウザのキャッシュをクリアします。

オプション	説明
既存のデータベース ファイルを使用してデータベースをリストア	バックアップが作成されたホストまたは別のホスト内にある代替SQL Serverにデータベースをリストアする場合は、このオプションを選択します。 指定した既存のファイル パスにデータベース ファイルが存在している必要があります。ホスト名を選択し、データベース名を入力し（オプション）、インスタンスを選択し、リストア パスを指定します。

7. [Recovery Scope]ページで、次のいずれかのオプションを選択します。

オプション	説明
None	ログなしで完全バックアップのみを復元する必要がある場合は、「なし」を選択します。
All log backups	完全バックアップ後に利用可能なすべてのログバックアップを復元するには、すべてのログ バックアップ 最新バックアップ復元操作を選択します。
By log backups until	ログ バックアップ別 を選択すると、ポイントインタイム復元操作が実行され、選択した日付のバックアップ ログまでのバックアップ ログに基づいてデータベースが復元されます。
By specific date until	復元されたデータベースにトランザクション ログが適用されなくなる日時を指定するには、[特定の日付まで] を選択します。 ポイントインタイム リストア処理では、指定した日時以降に記録されたトランザクション ログ エントリがリストアされません。

オプション	説明
Use custom log directory	すべてのログ バックアップ、ログ バックアップ 別、または*特定の日付まで*を選択し、ログがカスタムの場所に配置されている場合は、*カスタム ログ ディレクトリを使用する*を選択し、ログの場所を指定します。 カスタム ログ ディレクトリを使用する オプションは、データベースを別のホストに復元する または 既存のデータベース ファイルを使用してデータベースを復元する を選択した場合にのみ使用できます。共有パスを使用することもできますが、そのパスにSQLユーザがアクセスできるようにしてください。  カスタム ログ ディレクトリは、可用性グループ データベースではサポートされていません。

8. [Pre Ops]ページで、次の手順を実行します。

a. [Pre Restore Options]ページで、次のいずれかのオプションを選択します。

- 同じ名前のデータベースを復元するには、「復元中に同じ名前のデータベースを上書きする」を選択します。
- データベースを復元し、既存のレプリケーション設定を保持するには、「**SQL** データベースのレプリケーション設定を保持する」を選択します。
- 復元操作を開始する前にトランザクション ログを作成するには、[復元前にトランザクション ログのバックアップを作成する]を選択します。
- トランザクション ログ バックアップが失敗した場合に復元操作を中止するには、[復元前のトランザクション ログ バックアップが失敗した場合は復元を中止する]を選択します。

b. リストア ジョブの実行前に実行するオプションのスクリプトを指定します。

たとえば、SNMPトラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。



プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

9. [Post Ops]ページで、次の手順を実行します。

a. [Choose database state after restore completes]セクションで、次のいずれかのオプションを選択します。

- 必要なバックアップをすべて今すぐ復元する場合は、「操作可能、ただし追加のトランザクション ログの復元には使用できません」を選択します。

これはデフォルトの動作で、コミットされていないトランザクションをロールバックしてデータベースを使用可能な状態にします。バックアップを作成するまで追加のトランザクショ

ン ログはリストアできません。

- コミットされていないトランザクションをロールバックせずにデータベースを非操作状態のままにするには、「非操作状態ですが、追加のトランザクション ログの復元に使用できます」を選択します。

追加のトランザクション ログをリストアできます。データベースはリカバリされるまで使用できません。

- データベースを読み取り専用モードのままにするには、「追加のトランザクション ログを復元できる読み取り専用モード」を選択します。

コミットされていないトランザクションはロールバックされますが、ロールバックされた操作がスタンバイ ファイルに保存されるため、リカバリ前の状態に戻すことができます。

[Undo directory]オプションを有効にすると、トランザクション ログが追加でリストアされます。トランザクション ログのリストア処理が失敗した場合は、変更をロールバックすることができます。詳細については、SQL Serverのドキュメントを参照してください。

- b. リストア ジョブの実行後に実行するオプションのスクリプトを指定します。

たとえば、SNMPトラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。



プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

10. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。

11. 概要を確認し、[完了] をクリックします。

12. モニター > ジョブ ページを使用して復元プロセスを監視します。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよびGet-SmBackupReportコマンドレットを使用して、リストアする1つまたは複数のバックアップに関する情報を取得します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackupコマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId  
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269  
-Confirm:$false  
output:  
Name                : Restore  
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'  
Id                  : 2368  
StartTime           : 10/4/2016 11:22:02 PM  
EndTime            :  
IsCancellable       : False  
IsRestartable       : False  
IsCompleted         : False  
IsVisible           : True  
IsScheduled         : False  
PercentageCompleted : 0  
Description         :  
Status              : Queued  
Owner               :  
Error               :  
Priority             : None  
Tasks               : {}  
ParentJobID         : 0  
EventId             : 0  
JobTypeId           :  
ApisJobKey          :  
ObjectId            : 0  
PluginCode          : NONE  
PluginName          :
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

セカンダリ ストレージから**SQL Server**データベースのリストア

セカンダリ ストレージ システム上の物理LUN（RDM、iSCSI、またはFCP）から、バックアップされたSQL Serverデータベースをリストアすることができます。リストアは段階的に実施され、すべてのデータとログ ページがセカンダリ ストレージ システム上の指定したSQL Serverバックアップから指定したデータベースにコピーされます。

開始する前に

- プライマリ ストレージ システムからセカンダリ ストレージ システムにSnapshotをレプリケートしておく必要があります。

- SnapCenter Serverとプラグイン ホストがセカンダリ ストレージ システムに接続できることを確認しておく必要があります。
- [Restore]ウィザードの各ページのほとんどのフィールドについては、基本的なリストア プロセスで説明しています。以下の手順では、説明が必要な一部のフィールドを取り上げます。

タスク概要

SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotのロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから [SnapCenter Plug-in for SQL Server] を選択します。
2. [リソース] ページで、[表示] ドロップダウン リストから [データベース] または [リソース グループ] を選択します。
3. データベースまたはリソース グループを選択します。

データベースまたはリソース グループのトポロジ ページが表示されます。

4. [コピーの管理] セクションで、セカンダリ ストレージ システム (ミラーまたはボルト) から [バックアップ] を選択します。
5. リストからバックアップを選択し、クリックします .
6. [Location] ページで、選択したリソースをリストアするデスティネーション ボリュームを選択します。
7. 復元ウィザードを完了し、概要を確認して、[完了] をクリックします。

他のデータベースが共有している別のパスにデータベースをリストアした場合は、フル バックアップとバックアップ検証を実行して、リストアしたデータベースが物理レベルで破損していないことを確認してください。

PowerShellコマンドレットを使用したリソースのリストア

リソースのバックアップをリストアするときは、SnapCenter Serverとの接続セッションを開始し、バックアップをリストしてバックアップの情報を取得し、バックアップをリストアします。

PowerShellコマンドレットを実行できるように環境を準備しておく必要があります。

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよびGet-SmBackupReportコマンドレットを使用して、リストアする1つ

または複数のバックアップに関する情報を取得します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. Restore-SmBackupコマンドレットを使用して、バックアップからデータをリストアします。

```

Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime            :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :

```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

可用性グループ データベースの再シード

再シードは、可用性グループ（AG）データベースをリストアするためのオプションです。セカンダリ データベースがAG内のプライマリ データベースと同期していない場合は、セカンダリ データベースを再シードできます。

開始する前に

- リストアするセカンダリAGデータベースのバックアップを作成しておく必要があります。
- SnapCenter Serverとプラグイン ホストには、同じバージョンのSnapCenterがインストールされている必要があります。

タスク概要

- プライマリ データベースには再シード処理を実行できません。
- 可用性グループからレプリカ データベースが削除されると、再シード処理を実行できません。レプリカが削除されると、再シード処理は失敗します。
- SQL可用性グループ データベースで再シード処理を実行する際には、その可用性グループ データベースのレプリカ データベースでログ バックアップがトリガーされないようにしてください。再シード処理中にログ バックアップがトリガーされると、再シード処理は失敗し、「The mirror database, "database_name" has insufficient transaction log data to preserve the log backup chain of the principal database」というエラー メッセージが表示されます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから [SnapCenter Plug-in for SQL Server] を選択します。
2. [リソース] ページで、[表示] リストから [データベース] を選択します。
3. リストからセカンダリAGデータベースを選択します。
4. *再シード*をクリックします。
5. モニター > ジョブ をクリックして、操作の進行状況を監視します。

SQLリソースのリストア処理の監視

[Job]ページを使用して、SnapCenterの各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  でリストをフィルタリングし、リストア処理のみを表示します。
 - b. 開始日と終了日を指定します。

- c. *タイプ*ドロップダウンリストから*復元*を選択します。
 - d. *ステータス*ドロップダウンリストから、復元ステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. 復元ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
 5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

SQLリソースのリストア処理のキャンセル

キューに登録されているリストア ジョブはキャンセルできます。

リストア処理をキャンセルするには、SnapCenter管理者かジョブ所有者としてログインする必要があります。

タスク概要

- キューに入れられた復元操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のリストア処理はキャンセルできません。
- キューに登録されているリストア処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。
- キャンセルできない復元操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられた復元操作をキャンセルできます。

手順

次のいずれかを実行します。

方法	アクション
[Monitor]ページ	1. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 2. ジョブを選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	1. 復元操作を開始したら、 アクティビティ ペインで、最新の 5 つの操作を表示します。 2. 処理を選択します。 3. ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

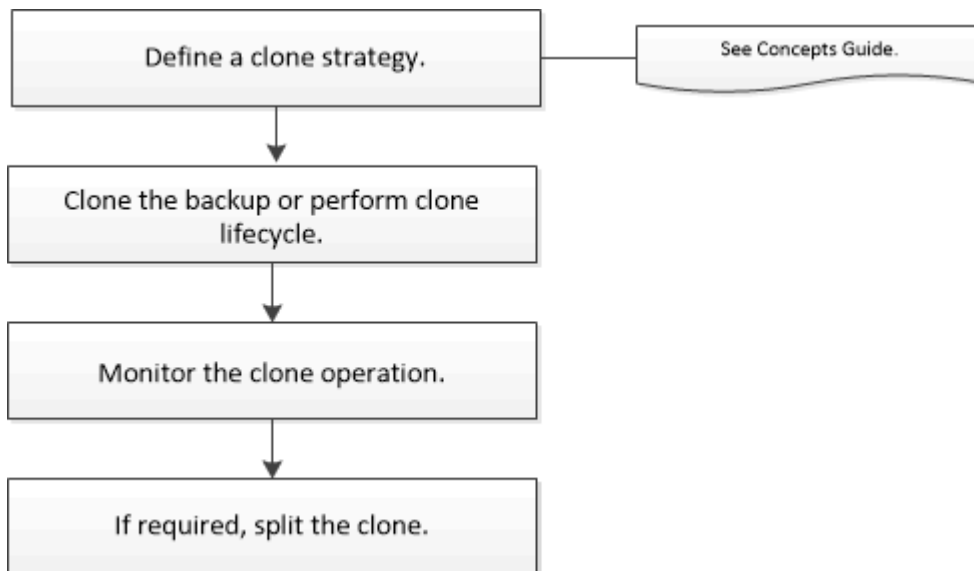
SQL Serverデータベース リソースのクローニング

クローニングのワークフロー

バックアップからデータベース リソースをクローニングする前に、SnapCenter Server でいくつかのタスクを実行する必要があります。データベースのクローニングは、本番環境のデータベースまたはそのバックアップ セットのポイントインタイム コピーを作成するプロセスです。アプリケーション開発サイクル中に実装が必要な機能を現在のデータベースの構造およびコンテンツを使用してテストする場合、データの抽出と操作を行うツールを使用してデータ ウェアハウスにデータを取り込む場合、誤って削除または変更されたデータをリカバリする場合などに実行します。

データベースのクローニング処理では、ジョブIDに基づいてレポートが生成されます。

次のワークフローは、クローニング処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、リカバリ、検証、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、[SnapCenter コマンドレットのヘルプを使用するか、"SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)

詳細情報

["SQL Serverデータベース バックアップからのクローニング"](#)

["クローン ライフサイクルの実行"](#)

["デフォルトのTCP_TIMEOUT値を使用すると、クローニング処理が失敗するか所要時間が長くなる場合がある"](#)

SQL Serverデータベース バックアップからのクローニング

SnapCenterを使用して、SQL Serverデータベース バックアップをクローニングすることができます。古いバージョンのデータに対してアクセスまたはリストアが必要な場合

は、データベース バックアップをオンデマンドでクローニングできます。

開始する前に

- データ保護の準備として、ホストの追加、リソースの特定、ストレージ システム接続の作成などのタスクを完了しておく必要があります。
- データベースまたはリソース グループをバックアップしておく必要があります。
- ログ バックアップを使用して代替ホストにクローニングする際に、セカンダリ ロケータを検出するには、mirror、vault、mirror-vaultなどのデータ保護タイプをデータLUNとログLUNで一致させる必要があります。
- SnapCenterのクローン処理中に、マウント済みのクローン ドライブが見つからない場合は、SnapCenter ServerのCloneRetryTimeoutパラメータを300に変更する必要があります。
- ボリュームをホストするアグリゲートがStorage Virtual Machine (SVM) の割り当て済みアグリゲート リストに含まれていることを確認します。

タスク概要

- スタンドアロン データベース インスタンスをクローニングする場合は、マウント ポイント パスが存在すること、および専用ディスクであることを確認してください。
- フェイルオーバー クラスタ インスタンス (FCI) をクローニングする場合は、マウント ポイントが存在すること、共有ディスクであること、およびパスとFCIが同じSQLリソース グループに属していることを確認してください。
- 各ホストに割り当てられているvFCイニシエータまたはFCイニシエータが1つだけであることを確認します。これは、SnapCenterでサポートされるイニシエータはホストごとに1つだけであるためです。
- ソース データベースまたはターゲット インスタンスがクラスタ共有ボリューム (CSV) 上にある場合、クローニングされたデータベースはCSV上に配置されます。
- SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.ConfigファイルにあるPredefinedWindowsScriptsDirectoryキーを使用して定義します。

必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

キーの値は、API を介して Swagger から表示できます: API /4.7/configsettings

GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。



仮想環境 (VMDK / RDM) の場合は、マウント ポイントが専用ディスクであることを確認してください。

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから [SnapCenter Plug-in for SQL Server] を選択します。
2. [リソース] ページで、[表示] リストから [データベース] または [リソース グループ] を選択します。



インスタンスのバックアップのクローニングはサポートされていません。

3. データベースまたはリソース グループを選択します。
4. コピーの管理 ビュー ページで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージ システムからバックアップを選択します。
5. バックアップを選択し、*を選択します。  *。
6. クローン オプション ページで、次のアクションを実行します。

フィールド	操作
Clone server	クローンをどのホスト上に作成するかを選択します。
Clone instance	データベース バックアップのクローニング先となるクローン インスタンスを選択します。 指定したクローン サーバ上のSQLインスタンスを選択する必要があります。
Clone suffix	クローン ファイル名に付加される、データベースがクローンであることを示すサフィックスを入力します。 たとえば、 <i>db1_clone</i> 。元のデータベースと同じ場所にクローニングする場合、クローニングされたデータベースを元のデータベースと区別するためにサフィックスを指定する必要があります。そうしないと、処理が失敗します。

フィールド	操作
Auto assign mount point / Auto assign volume mount point under path	マウント ポイントを自動的に割り当てるか、またはパスを指定してボリューム マウント ポイントを自動的に割り当てるかを選択します。 パスの下ボリューム マウント ポイントを自動割り当て: パスの下のマウント ポイントを使用すると、特定のディレクトリを提供できます。指定したディレクトリにマウント ポイントが作成されます。このオプションを選択する場合は、ディレクトリが空であることを事前に確認しておく必要があります。ディレクトリにデータベースが格納されている場合、そのデータベースはマウント処理後に無効な状態になります。

7. [Logs]ページで、次のいずれかのオプションを選択します。

フィールド	操作
None	ログなしでフル バックアップのみをクローニングする場合は、このオプションを選択します。
All log backups	フル バックアップ後の日付のログ バックアップをすべてクローニングする場合、このオプションを選択します。
By log backups until	選択した日付のバックアップ ログまでのバックアップ ログに基づいてデータベースをクローニングする場合、このオプションを選択します。
By specific date until	クローニングされたデータベースにトランザクション ログを適用する最終日時を指定します。 このポイントインタイムのクローニングでは、指定した日時以降に記録されたトランザクション ログ エントリがクローニングされません。

8. スクリプト ページで、スクリプトのタイムアウト、パス、およびクローン操作の前または後に実行するプレスクリプトまたはポストスクリプトの引数をそれぞれ入力します。

たとえば、SNMPトラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。



プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

デフォルトのスクリプト タイムアウトは60秒です。

9. *通知*ページの*電子メール設定*ドロップダウンリストから、電子メールを送信するシナリオを選択

します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。実行されたクローン操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtplibServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

EMSについては、["EMSデータ収集の管理"](#)

10. 概要を確認し、[完了] を選択します。

11. モニター > ジョブ を選択して、操作の進行状況を監視します。

終了後の操作

クローンの作成後は、名前を変更しないでください。

関連情報

["デフォルトのTCP_TIMEOUT値を使用すると、クローニング処理が失敗するか所要時間が長くなる場合がある"](#)

["フェイルオーバー クラスター インスタンスのデータベース クローニングが失敗する"](#)

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. クローニングできるバックアップの一覧を表示するには、Get-SmBackupコマンドレットかGet-SmResourceGroupコマンドレットを使用します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

この例では、指定したリソース グループとそのリソース、および関連ポリシーに関する情報を表示しています。

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :  
CreationTime : 8/4/2015 3:44:05 PM  
ModificationTime : 8/4/2015 3:44:05 PM  
EnableEmail : False  
EmailSMTPServer :  
EmailFrom :  
EmailTo :  
EmailSubject :  
EnableSysLog : False  
ProtectionGroupType : Backup  
EnableAsupOnFailure : False  
Policies : {FinancePolicy}  
HostResourceMapping : {}  
Configuration : SMCoreContracts.SmCloneConfiguration  
LastBackupStatus :  
VerificationServer :  
EmailBody :  
EmailNotificationPreference : Never  
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo  
SchedulerSQLInstance :  
CustomText :  
CustomSnapshotFormat :  
SearchResources : False  
ByPassCredential : False  
IsCustomSnapshot :  
MaintenanceStatus : Production  
PluginProtectionGroupTypes : {SMSQL}  
Name : Payrolldataset  
Type : Group  
Id : 1  
Host :  
UserName :  
Passphrase :  
Deleted : False  
Auth : SMCoreContracts.SmAuth  
IsClone : False  
CloneLevel : 0  
ApplySnapvaultUpdate : False  
ApplyRetention : False  
RetentionCount : 0  
RetentionDays : 0  
ApplySnapMirrorUpdate : False  
SnapVaultLabel :
```


MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False

```
Auth : SMCoreContracts.SmAuth  
IsClone : False
```

3. 既存のバックアップからのクローニング処理を開始するには、New-SmCloneコマンドレットを使用します。

この例では、指定したバックアップからすべてのログを含めてクローンを作成しています。

```
PS C:\> New-SmClone  
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774  
-Resources @{"Host"="vise-f3.sddev.mycompany.com";  
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}  
-CloneToInstance vise-f3\squlexpress -AutoAssignMountPoint  
-Suffix _clonefrombackup  
-LogRestoreType All -Policy clonefromprimary_ondemand  
  
PS C:\> New-SmBackup -ResourceGroupName PayrollDataset -Policy  
FinancePolicy
```

この例では、指定したMicrosoft SQL Serverインスタンスのクローンを作成しています。

```
PS C:\> New-SmClone  
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"  
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";  
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}  
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"  
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. クローニング ジョブのステータスを表示するには、Get-SmCloneReportコマンドレットを使用します。

この例では、指定したジョブIDのクローン レポートを表示しています。

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

クローン ライフサイクルの実行

SnapCenterを使用して、リソース グループまたはデータベースからクローンを作成できます。クローニングはオンデマンドで実行することも、リソース グループまたはデータベースに対して定期的なクローニング処理をスケジュール設定することもできます。バックアップを定期的にクローニングすると、クローンを使用してアプリケーションの開発、データの取り込み、またはデータのリカバリを行うことができます。

SnapCenterでは、複数のサーバで同時に複数のクローニング処理を実行するようにスケジュールを設定できます。

開始する前に

- スタンドアロン データベース インスタンスをクローニングする場合は、マウント ポイント パスが存在すること、および専用ディスクであることを確認してください。
- フェイルオーバー クラスタ インスタンス (FCI) をクローニングする場合は、マウント ポイントが存在すること、共有ディスクであること、およびパスとFCIが同じSQLリソース グループに属していることを確認してください。
- ソース データベースまたはターゲット インスタンスがクラスタ共有ボリューム (CSV) 上にある場合、クローニングされたデータベースはCSV上に配置されます。



仮想環境（VMDK / RDM）の場合は、マウント ポイントが専用ディスクであることを確認してください。

タスク概要

- SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.ConfigファイルにあるPredefinedWindowsScriptsDirectoryキーを使用して定義します。

必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

キーの値は、API を介して Swagger から表示できます: API /4.7/configsettings

GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。

- [Clone lifecycle]ウィザードの各ページのフィールドのほとんどはわかりやすいもので、説明を必要としません。以下の手順では、説明が必要なフィールドを取り上げます。
- ONTAP 9.12.1以前のバージョンでは、Snapshotのロック期間を指定すると、改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

- 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
- [リソース] ページで、[表示] リストから [データベース] または [リソース グループ] を選択します。
- リソース グループまたはデータベースを選択し、[ライフサイクルの複製] をクリックします。
- [Options]ページで、次の操作を実行します。

フィールド	操作
Clone job name	クローン ライフサイクル ジョブに、ジョブを監視および変更する際にわかりやすい名前を指定します。
Clone server	クローンをどのホストに配置するかを選択します。
Clone instance	データベースのクローニング先となるクローン インスタンスを選択します。指定したクローン サーバ上のSQLインスタンスを選択する必要があります。

フィールド	操作
Clone suffix	クローン データベースに付加される、データベースがクローンであることを示すサフィックスを入力します。クローン リソース グループの作成に使用する各SQLインスタンスには、一意なデータベース名が必要です。たとえば、クローン リソース グループに SQL インスタンス “inst1” からのソース データベース “db1” が含まれており、“db1” が “inst1” にクローンされている場合、クローン データベース名は “db1clone” になります。データベースは同じインスタンスに複製されるため、「clone」は必須のユーザー定義サフィックスです。「db1」が SQL インスタンス 「inst2」 にクローンされる場合、データベースは別のインスタンスにクローンされるため、クローン データベース名は「db1」のままになります (サフィックスはオプションです)。
Auto assign mount point / Auto assign volume mount point under path	マウント ポイントを自動的に割り当てるか、またはパスを指定してボリューム マウント ポイントを自動的に割り当てるかを選択します。[Auto assign volume mount point under path]を選択した場合は、ディレクトリを指定できます。指定したディレクトリにマウント ポイントが作成されます。このオプションを選択する場合は、ディレクトリが空であることを事前に確認しておく必要があります。ディレクトリにデータベースが格納されている場合、そのデータベースはマウント処理後に無効な状態になります。

5. [Location]ページで、クローンを作成するストレージの場所を選択します。
6. [Script]ページで、クローニング処理の前またはあとに実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

たとえば、SNMPトラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。



プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

デフォルトのスクリプト タイムアウトは60秒です。

7. [Schedule]ページで、次のいずれかを実行します。
 - クローンジョブをすぐに実行するには、[今すぐ実行] を選択します。
 - クローン操作を実行する頻度、クローン スケジュールを開始する日時、クローン操作を実行する日、スケジュールの有効期限、スケジュールの有効期限が切れた後にクローンを削除するかどうかを決定する場合は、[スケジュールの構成] を選択します。
8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。実行され

たクローン操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

EMSについては、"[EMSデータ収集の管理](#)"

9. 概要を確認し、[完了] をクリックします。

モニター > ジョブ ページを使用して、クローン作成プロセスを監視する必要があります。

SQLデータベースのクローニング処理の監視

SnapCenterのクローニング処理の進捗状況を、[Jobs]ページで監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録
- キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし てリストをフィルタリングし、クローニング処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*クローン*を選択します。
 - d. *ステータス*ドロップダウンリストからクローンのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. クローンジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. ジョブの詳細ページで、*ログの表示*をクリックします。

SQLリソースのクローニング処理のキャンセル

キューに登録されているクローニング処理はキャンセルできます。

クローニング処理をキャンセルするには、SnapCenter管理者かジョブ所有者としてログインする必要があります。

タスク概要

- キューに入れられたクローン操作は、モニター ページまたは アクティビティ ペインからキャンセルできます。
- 実行中のクローニング処理はキャンセルできません。
- キューに登録されているクローニング処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたクローン操作をキャンセルできます。

手順

次のいずれかを実行します。

方法	アクション
[Monitor]ページ	1. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 2. 操作を選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	1. クローン操作を開始したら、 アクティビティ ペインで、最新の 5 つの操作を表示します。 2. 処理を選択します。 3. *ジョブの詳細* ページで、*ジョブのキャンセル* をクリックします。

クローンのスプリット

SnapCenterを使用して、クローン リソースを親リソースからスプリットできます。スプリットされたクローンは親リソースから独立します。

タスク概要

- 中間クローンではクローン スプリット処理を実行できません。

たとえば、データベース バックアップからクローン1を作成したあとで、クローン1のバックアップを作成し、そのバックアップ（クローン2）をクローニングできます。クローン2を作成すると、クローン1は中間クローンになり、クローン1ではクローン スプリット処理を実行できなくなります。ただし、クローン2に対してはクローン スプリット処理を実行できます。

クローン2をスプリットすると、クローン1は中間クローンではなくなるため、クローン1に対してクローン スプリット処理を実行できるようになります。

- クローンをスプリットすると、そのクローンのバックアップ コピーとクローン ジョブが削除されます。
- FlexCloneボリューム分割操作の詳細については、以下を参照してください。 ["親ボリュームからのFlexCloneボリュームのスプリット"](#)。
- ストレージ システム上のボリュームまたはアグリゲートがオンラインであることを確認します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. *リソース*ページで、表示リストから適切なオプションを選択します。

オプション	説明
データベース アプリケーションの場合	表示リストから*データベース*を選択します。
ファイルシステムの場合	表示リストから*パス*を選択します。

3. リストから適切なリソースを選択します。

リソースのトポロジ ページが表示されます。

4. *コピーの管理*ビューから、クローンされたリソース（データベースやLUNなど）を選択し、*をクリックします。  *。
5. 分割するクローンの推定サイズとアグリゲート上で必要な空き容量を確認し、[開始] をクリックします。
6. モニター > ジョブ をクリックして、操作の進行状況を監視します。

SMCoreサービスが再起動されると、クローン スプリット処理は応答を停止します。Stop-SmJobコマンドレットを実行してクローン スプリット処理を停止してから、クローン スプリット処理を再試行してください。

クローンが分割されているかどうかを確認するためのポーリング時間を長くしたり短くしたりする場合は、SMCoreServiceHost.exe.config ファイルの CloneSplitStatusCheckPollTime パラメータの値を変更して、SMCore がクローン分割操作のステータスをポーリングする時間間隔を設定できます。値はミリ秒単位で、デフォルト値は5分です。

例えば：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

バックアップ、リストア、または別のクローン スプリットが実行中の場合、クローン スプリットの開始処理は失敗します。クローン スプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

["アグリゲートが存在しないためにSnapCenterのクローニングや検証が失敗する"](#)

SAP HANAデータベースの保護

SnapCenter Plug-in for SAP HANA Database

SnapCenter Plug-in for SAP HANA Databaseの概要

SnapCenter Plug-in for SAP HANA Databaseは、SAP HANAデータベースに対応したデータ保護管理を提供する、NetApp SnapCenterソフトウェアのホスト側コンポーネントです。Plug-in for SAP HANA Databaseは、SnapCenter環境でのSAP HANAデータベースのバックアップ、リストア、およびクローニングを自動化します。

SnapCenterは、単一コンテナとマルチテナント データベース コンテナ（MDC）をサポートします。Plug-in for SAP HANA Databaseは、WindowsとLinuxのどちらの環境でも使用できます。HANAデータベース ホストにインストールされていないプラグインは、一元化されたホスト プラグインと呼ばれます。一元化されたホスト プラグインでは、異なるホストにまたがる複数のHANAデータベースを管理できます。

Plug-in for SAP HANA Databaseがインストールされている場合は、SnapCenterとNetApp SnapMirrorテクノロジーを使用して、バックアップ セットのミラー コピーを別のボリュームに作成できます。また、このプラグインをNetApp SnapVaultテクノロジーとともに使用して、標準への準拠を目的としたディスクツーディスク バックアップ レプリケーションを実行することもできます。

SAP HANA データベース用プラグインは、サイト全体の障害時でもビジネス サービスの運用を継続できるようにするSnapMirrorアクティブ シンク (当初はSnapMirror Business Continuity [SM-BC] としてリリース) をサポートし、セカンダリ コピーを使用してアプリケーションを透過的にフェイルオーバーできるようにします。SnapMirrorアクティブ同期でフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。

SnapCenter Plug-in for SAP HANA Databaseの機能

環境に SAP HANA データベース用プラグインをインストールすると、SnapCenterを使用して SAP HANA データベースとそのリソースをバックアップ、復元、および複製できます。これらの処理をサポートするタスクも実行できます。

- データベースを追加します。
- バックアップを作成します。
- バックアップからリストアします。
- バックアップをクローニングします。
- バックアップ処理のスケジュールを設定します。
- バックアップ、リストア、クローニングの各処理を監視します。
- バックアップ、リストア、クローニングの各処理のレポートを表示します。

SnapCenter Plug-in for SAP HANA Databaseの特長

SnapCenterは、プラグイン アプリケーションと統合されるほか、ストレージ システム上でNetAppの数々のテクノロジーと統合されます。Plug-in for SAP HANA Databaseの操

作には、SnapCenterのグラフィカル ユーザ インターフェイスを使用します。

- 統合されたグラフィカルユーザーインターフェース

SnapCenterのインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。どのプラグインでも、SnapCenterのインターフェイスから、バックアップ、リストア、クローニングの各処理を一貫した方法で実行できるほか、ダッシュボード ビューで概要を把握したり、ロールベース アクセス制御（RBAC）を設定したり、ジョブを監視したりすることができます。

- 自動化された中央管理

バックアップ処理のスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理を実行したりできます。SnapCenterからのEメール アラートの送信を設定して、環境をプロアクティブに監視することもできます。

- 無停止の**NetApp**スナップショットコピーテクノロジー

SnapCenterでは、Plug-in for SAP HANA DatabaseでNetApp Snapshotテクノロジーを使用してリソースがバックアップされます。

Plug-in for SAP HANA Databaseを使用すると、次のメリットもあります。

- バックアップ、リストア、およびクローニングのワークフローがサポートされます。
- セキュリティがRBACでサポートされ、ロール委譲が一元化されます。

クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルのアクセス権を付与することもできます。

- NetApp FlexCloneテクノロジーを使用して、テストまたはデータ抽出に使用するリソースのコピー（スペース効率に優れたポイントインタイム コピー）を作成できます。

クローンを作成するストレージ システムにFlexCloneライセンスが必要です。

- バックアップの作成でONTAPの整合グループ（CG）のSnapshot機能がサポートされます。
- 複数のリソース ホストで同時に複数のバックアップを実行できます。

1回の処理で、1つのホストの複数のリソースが同じボリュームを共有する場合に複数のSnapshotが統合されます。

- 外部コマンドを使用してSnapshotを作成できます。
- ファイルベースのバックアップがサポートされます。
- XFSファイルシステム上のLinux LVMがサポートされます。

SnapCenter Plug-in for SAP HANA Databaseでサポートされるストレージ タイプ

SnapCenterは、物理マシンと仮想マシン（VM）の両方でさまざまなストレージ タイプをサポートしています。SnapCenter Plug-in for SAP HANA Databaseをインストールする前に、ストレージ タイプがサポートされているかどうかを確認する必要があります。

マシン	ストレージ タイプ
物理サーバ	• FC接続LUN • iSCSI接続LUN • NFS接続ボリューム
VMware ESXi	• FCまたはiSCSI HBAで接続されたRDM LUNホスト バス アダプタ (HBA) のスキャン は、SnapCenterがホストに存在するすべてのホスト バス アダプタをスキャンするため、完了までに時間がかかることがあります。 <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> にある LinuxConfig.pm ファイルを編集し て、SCSI_HOSTS_OPTIMIZED_RESCAN パラメータの値を 1 に設定し、HBA_DRIVER_NAMES にリストされているHBA のみを再スキャンすることができます。 • iSCSIイニシエータでゲスト システムに直接接続されたiSCSI LUN • NFSデータストア上のVMDK • VMFS上にVMDKが作成されました • ゲスト システムに直接接続されたNFSボリューム • NFSとSANの両方に存在するvVolデータストア vVolデータストアは、ONTAP Tools for VMware vSphereでのみプロビジョニングできます。

SAP HANA プラグインに必要な最小ONTAP権限

必要な最小ONTAP権限は、データ保護に使用するSnapCenterプラグインによって異なります。

- 全アクセス コマンド: ONTAP 9.12.1 以降に必要な最小限の権限
 - event generate-autosupport-log
 - job history show
 - job stop
 - lun
 - lun create
 - lun create

- lun create
- lun delete
- lun igroup add
- lun igroup create
- lun igroup delete
- lun igroup rename
- lun igroup rename
- lun igroup show
- lun mapping add-reporting-nodes
- lun mapping create
- lun mapping delete
- lun mapping remove-reporting-nodes
- lun mapping show
- lun modify
- lun move-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- lun resize
- lun serial
- lun show
- snapmirror policy add-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- snapmirror restore
- snapmirror show
- snapmirror show-history
- snapmirror update
- snapmirror update-ls-set
- snapmirror list-destinations
- version
- volume clone create
- volume clone show
- volume clone split start
- volume clone split stop
- volume create

- volume destroy
- volume file clone create
- volume file show-disk-usage
- volume offline
- volume online
- volume modify
- volume qtree create
- volume qtree delete
- volume qtree modify
- volume qtree show
- volume restrict
- volume show
- volume snapshot create
- volume snapshot delete
- volume snapshot modify
- volume snapshot modify-snaplock-expiry-time
- volume snapshot rename
- volume snapshot restore
- volume snapshot restore-file
- volume snapshot show
- volume unmount
- vservers cifs
- vservers cifs share create
- vservers cifs share delete
- vservers cifs shadowcopy show
- vservers cifs share show
- vservers cifs show
- vservers export-policy
- vservers export-policy create
- vservers export-policy delete
- vservers export-policy rule create
- vservers export-policy rule show
- vservers export-policy show
- vservers iscsi
- vservers iscsi connection show
- vservers show

- 読み取り専用コマンド: ONTAP 8.3.0以降に必要な最小限の権限

- ネットワークインターフェース
- network interface show
- SVM

SAP HANAデータベースでのSnapMirrorレプリケーションとSnapVaultレプリケーションのためのストレージ システムの準備

SnapCenterプラグインと一緒にONTAP SnapMirrorテクノロジーを使用すると、バックアップセットのミラー コピーを別のボリュームに作成できます。また、ONTAP SnapVaultを使用すれば、標準への準拠やその他のガバナンスを目的としたディスクツリー ディスクのバックアップ レプリケーションを実行できます。これらのタスクを実行する前に、ソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenterは、Snapshot処理の完了後に、SnapMirrorとSnapVaultに対する更新を実行します。SnapMirror更新とSnapVault更新は、SnapCenterジョブの一部として実行されるため、ONTAPスケジュールを別途作成しないでください。



NetApp SnapManager製品からSnapCenterに移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリ ストレージ（ソース ボリューム）上のデータがセカンダリ ストレージ（デスティネーション ボリューム）にレプリケートされます。この関係を初期化すると、ソース ボリュームで参照されるデータ ブロックがデスティネーション ボリュームに転送されます。



SnapCenter は、SnapMirrorとSnapVaultボリューム間のカスケード関係をサポートしていません（* プライマリ * > ミラー > ボールト）。ファンアウト関係を使用する必要があります。

SnapCenterは、バージョンに依存しないSnapMirror関係の管理をサポートしています。バージョンに依存しないSnapMirror関係とその設定方法の詳細については、["ONTAPのドキュメント"](#)。

SAP HANAデータベースのバックアップ戦略

SAP HANAデータベースのバックアップ戦略の定義

バックアップ ジョブを作成する前にバックアップ戦略を定義しておく、リソースの正常なリストアやクローニングに必要なバックアップを作成するのに役立ちます。バックアップ戦略の大部分は、サービス レベル アグリーメント（SLA）、目標復旧時間（RTO）、および目標復旧時点（RPO）によって決まります。

タスク概要

SLAとは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。RTOは、サービスの停止からビジネス プロセスの復旧までに必要となる時間です。RPOは、障害発生後に通常処理を再開するためにバックアップ ストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA、RTO、およびRPOは、データ保護戦略に関与します。

手順

1. リソースをバックアップするタイミングを決定します。
2. 必要なバックアップ ジョブの数を決定します。
3. バックアップの命名方法を決定します。
4. Snapshotコピーベースのポリシーを作成してアプリケーションと整合性のあるデータベースのSnapshotをバックアップするかどうかを決定します。
5. データベースの整合性を検証するかどうかを決定します。
6. レプリケーションのためにNetApp SnapMirrorテクノロジーを使用するか、または長期保持のためにNetApp SnapVaultテクノロジーを使用するかを決定します。
7. ソース ストレージ システムおよびSnapMirrorデスティネーションでのSnapshotの保持期間を確認します。
8. バックアップ処理の前後にコマンドを実行するかどうかを決定し、実行する場合はプリスクリプトまたはポストスクリプトを用意します。

Linuxホスト上のリソースの自動検出

リソースとは、SnapCenterで管理するLinuxホスト上のSAP HANAデータベースとデータ ボリューム以外のボリュームです。SnapCenter Plug-in for SAP HANA Databaseプラグインをインストールすると、そのLinuxホスト上のSAP HANAデータベースが自動的に検出されて[Resources]ページに表示されます。

自動検出は、次のSAP HANAリソースでサポートされています。

- 単一のコンテナ

プラグインのインストールまたはアップグレード後、一元化されたホスト プラグインにある単一コンテナリソースは、手動で追加したリソースとして引き続き扱われます。

プラグインをインストールまたはアップグレードすると、SnapCenterに直接登録されているSAP HANA LinuxホストでのみSAP HANAデータベースが自動的に検出されます。

- マルチテナント データベース コンテナ (MDC)

プラグインのインストールまたはアップグレード後、一元化されたホスト プラグインにあるMDCリソースは、手動で追加したリソースとして引き続き扱われます。

SnapCenter 4.3にアップグレードしたあとも、MDCリソースは一元化されたホスト プラグインに手動で追加する必要があります。

SnapCenterに直接登録されているSAP HANA Linuxホストの場合、プラグインをインストールまたはアップグレードすると、ホスト上のリソースの自動検出がトリガーされます。プラグインをアップグレードすると、プラグイン ホストに配置されていたMDCリソースそれぞれが、別のGUID形式を持つ別のMDCリソースとして自動的に検出され、SnapCenterに登録されます。新しいリソースはロック状態になります。

たとえば、SnapCenter 4.2で、E90 MDCリソースがプラグイン ホストにあり、手動で登録されていた場合、SnapCenter 4.3へのアップグレード後には、異なるGUIDを持つ別のE90 MDCリソースが検出されてSnapCenterに登録されます。

自動検出は、次の構成ではサポートされていません。

- RDMおよびVMDKレイアウト



上記のリソースが検出された場合、これらのリソースではデータ保護処理がサポートされません。

- HANAマルチホスト構成
- 同じホスト上の複数のインスタンス
- マルチティア スケールアウトHANAシステム レプリケーション
- システム レプリケーション モードのカスケード レプリケーション環境

サポートされるバックアップのタイプ

バックアップ タイプでは、作成するバックアップのタイプを指定します。SnapCenterでは、SAP HANAデータベースについて、ファイルベースのバックアップとSnapshotコピーベースのバックアップをサポートしています。

ファイルベースのバックアップ

ファイルベースのバックアップでは、データベースの整合性が検証されます。ファイルベースのバックアップの処理は一定の間隔で実行するようにスケジュールを設定できます。アクティブなテナントのみがバックアップされます。ファイルベースのバックアップはSnapCenterでリストアまたはクローニングすることはできません。

Snapshotコピーベースのバックアップ

Snapshotコピーベースのバックアップでは、NetApp Snapshotテクノロジーを利用して、SAP HANAデータベースが格納されたボリュームのオンラインの読み取り専用のコピーが作成されます。

SnapCenter Plug-in for SAP HANA Databaseでの整合グループSnapshotの使用方法

プラグインを使用して、リソース グループの整合グループSnapshotを作成することができます。整合グループとはボリュームのコンテナであり、複数のボリュームを格納して1つのエンティティとして管理できます。整合グループには複数のボリュームの同時に作成されたSnapshotが格納されるため、一連のボリュームのコピーの整合性が確保されます。

ストレージ コントローラが整合性を確保しながらSnapshotをグループ化するのを待機する時間も指定できます。利用可能な待機時間のオプションは、「緊急」、「中」、「緩和」です。また、整合グループSnapshotの処理でWrite Anywhere File Layout (WAFL) の同期を有効にするか無効にするかも選択できます。WAFLの同期を有効にすると、整合グループSnapshotのパフォーマンスが向上します。

SnapCenterによる不要なログおよびデータ バックアップの削除の管理

ストレージ システム レベルおよびファイルシステム レベルでの不要なログおよびデータ バックアップの削除は、SAP HANAのバックアップ カタログ内のエントリも含め、SnapCenterで管理されます。

保持設定に基づいて、プライマリ ストレージまたはセカンダリ ストレージのSnapshotが削除され、SAP

HANAのカatalog内の対応するエントリも削除されます。SAP HANAのカatalogのエントリは、バックアップやリソース グループを削除したときにも削除されます。

SAP HANAデータベースのバックアップ スケジュールを決定する際の考慮事項

バックアップのスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率です。使用頻度の高いリソースは1時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは1日に1回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービス レベル アグリーメント（SLA）、目標復旧時点（RPO）などがあります。

バックアップ スケジュールには、次の2つの要素があります。

- バックアップ頻度（バックアップを実行する間隔）

バックアップ頻度は、ポリシー設定の一部であり、一部のプラグインではスケジュール タイプとも呼ばれます。たとえば、毎時、毎日、毎週、または毎月としてバックアップ頻度を設定できます。

- バックアップ スケジュール（バックアップが実行される日時）

バックアップ スケジュールは、リソースまたはリソース グループの設定の一部です。たとえば、週次バックアップのポリシーが設定されているリソースグループがある場合、毎週木曜日の午後10時にバックアップするようにスケジュールを設定できます。

SAP HANAデータベースの必要なバックアップ ジョブの数

必要なバックアップ ジョブの数を左右する要因としては、リソースのサイズ、使用中のボリュームの数、リソースの変更率、サービス レベル アグリーメント（SLA）などがあります。

Plug-in for SAP HANAデータベースのバックアップの命名規則

Snapshotのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則ではSnapshot名にタイムスタンプが追加されるので、コピーが作成されたタイミングを特定できます。

Snapshotでは、次のデフォルトの命名規則が使用されます。

resourcegroupname_hostname_timestamp

バックアップ リソース グループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- *dts1* はリソース グループ名です。

- `mach1x88` はホスト名です。
- `03-12-2015_23.17.26` は日付とタイムスタンプです。

または、[スナップショット コピーにカスタム名形式を使用する] を選択して、リソースまたはリソース グループを保護しながらスナップショット名の形式を指定することもできます。たとえば、`customtext_resourcegroup_policy_hostname`や`resourcegroup_hostname`などの形式です。デフォルトでは、Snapshot名にタイムスタンプのサフィックスが追加されます。

SAP HANAデータベースのリストアとリカバリの戦略

SAP HANAリソースのリストアとリカバリの戦略の定義

データベースのリストアとリカバリを行う前に戦略を定義しておく、リストア処理とリカバリ処理を正常に実行できるようになります。

手順

1. 手動で追加したSAP HANAリソースでサポートされるリストア戦略を確認します。
2. 自動検出されたSAP HANAデータベースでサポートされるリストア戦略を確認します。
3. 実行するリカバリ処理のタイプを決定します。

手動で追加した**SAP HANA**リソースでサポートされるリストア戦略のタイプ

SnapCenterを使用してリストア処理を正常に実行するには、戦略を定義しておく必要があります。手動で追加したSAP HANAリソースには、2種類のリストア戦略があります。手動で追加したSAP HANAリソースはリカバリできません。



手動で追加したSAP HANAリソースはリカバリできません。

リソース全体のリストア

- リソースのすべてのボリューム、qtree、およびLUNをリストア



リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeのリストア用のSnapshotが選択されたあとに作成されたSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。

ファイルレベルのリストア

- ボリューム、qtree、またはディレクトリからファイルをリストア
- 選択したLUNのみをリストア

自動検出された**SAP HANA**データベースでサポートされるリストア戦略のタイプ

SnapCenterを使用してリストア処理を正常に実行するには、戦略を定義しておく必要があります。自動検出されたSAP HANAデータベースには、2種類のリストア戦略があります。

リソース全体のリストア

- リソースのすべてのボリューム、qtree、およびLUNをリストア
 - ボリューム全体を復元するには、「ボリュームを元に戻す」オプションを選択する必要があります。



リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeのリストア用のSnapshotが選択されたあとに作成されたSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。

テナント データベース

- テナント データベースのリストア

テナント データベース オプションを選択した場合は、リカバリ操作を実行するために、SnapCenter外部のHANA スタジオまたは HANA リカバリ スクリプトを使用する必要があります。

自動検出された**SAP HANA**データベースのリストア処理のタイプ

SnapCenterでは、自動検出されたSAP HANAデータベースに対して、ボリュームベースのSnapRestore (VBSR)、Single File SnapRestore、およびConnect and Copyリストアのリストア タイプがサポートされます。

NFS環境でボリュームベースのSnapRestore (VBSR) を実行するシナリオは、次のとおりです。

- 復元対象として選択されたバックアップがSnapCenter 4.3より前のリリースで作成され、**Complete Resource**オプションが選択されている場合のみ
- 復元対象として選択されたバックアップがSnapCenter 4.3で作成され、*ボリュームの復元*オプションが選択されている場合

NFS環境でSingle File SnapRestoreを実行するシナリオは、次のとおりです。

- 復元対象として選択されたバックアップがSnapCenter 4.3で作成され、*完全なリソース*オプションのみが選択された場合
- マルチテナント データベース コンテナ (MDC) の場合、復元用に選択されたバックアップがSnapCenter 4.3 で取得され、テナント データベース オプションが選択されている場合
- 選択したバックアップがSnapMirrorまたはSnapVaultのセカンダリロケーションからのものであり、*完全なリソース*オプションが選択されている場合

SAN環境でSingle File SnapRestoreを実行するシナリオは、次のとおりです。

- SnapCenter 4.3より前のリリースでバックアップが取られ、*完全なリソース*オプションが選択されている場合のみ
- SnapCenter 4.3でバックアップが取られ、*完全なリソース*オプションが選択されている場合のみ
- バックアップがSnapMirrorまたはSnapVaultのセカンダリロケーションから選択され、*完全なリソース*オプションが選択されている場合

SAN環境でConnect and Copyリストアを実行するシナリオは、次のとおりです。

- MDCの場合、復元対象として選択されたバックアップがSnapCenter 4.3で取得され、*テナントデータベース*オプションが選択されている場合



復元スコープ ページで、完全なリソース、ボリュームの復元、および テナント データベース オプションを使用できます。

SAP HANAデータベースでサポートされるリカバリ処理のタイプ

SnapCenterでは、SAP HANAデータベースに対してさまざまなタイプのリカバリ処理を実行できます。

- データベースを最新の状態までリカバリする
- データベースを特定の時点までリカバリする

リカバリの日時を指定する必要があります。

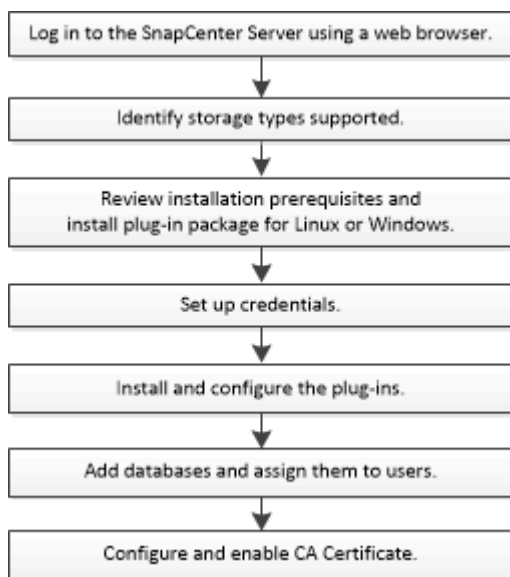
- データベースを特定のデータ バックアップまでリカバリする

SnapCenterでは、SAP HANAデータベースに対して[No recovery]オプションも選択できます。

SnapCenter Plug-in for SAP HANA Databaseのインストール準備

SnapCenter Plug-in for SAP HANA Databaseのインストール ワークフロー

SAP HANA データベースを保護する場合は、SAP HANA データベース用のSnapCenter プラグインをインストールして設定する必要があります。



ホストを追加して**SnapCenter Plug-in for SAP HANA Database**をインストールするための前提条件

ホストを追加してプラグイン パッケージをインストールする前に、すべての要件を満たしておく必要があります。SnapCenter Plug-in for SAP HANA Databaseは、Windows とLinuxどちらの環境でも使用できます。

- Java 11をホストにインストールしておく必要があります。



IBM Java は Windows および Linux ホストではサポートされていません。

- SAP HANAデータベースの対話型端末（HDBSQLクライアント）をホストにインストールしておく必要があります。
- Windows の場合、プラグイン クリエーター サービスは、"LocalSystem` Windows ユーザーを使用して実行する必要があります。これは、SAP HANA データベース用プラグインがドメイン管理者としてインストールされている場合のデフォルトの動作です。
- Windowsの場合は、ユーザ ストア キーをSYSTEMユーザとして作成する必要があります。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。WindowsホストにSAP HANAプラグインをインストールすると、SnapCenter Plug-in for Microsoft Windowsもデフォルトで導入されます。
- Linuxホストの場合は、HDB Secure User StoreのキーにはHDBSQL OSユーザとしてアクセスします。
- SnapCenter Serverが、Plug-in for SAP HANA Databaseホストの8145ポートまたはカスタム ポートにアクセスする必要があります。

Windowsホスト

- ローカル管理者権限があり、リモート ホストに対してローカル ログインのアクセス許可があるドメイン ユーザが必要です。
- Plug-in for SAP HANA DatabaseをWindowsホストにインストールすると、SnapCenter Plug-in for Microsoft Windowsが自動的にインストールされます。
- rootユーザまたはroot以外のユーザに対してパスワード ベースのSSH接続を有効にしておく必要があります。
- Java 11をWindowsホストにインストールしておく必要があります。

["すべてのオペレーティングシステム用のJAVAをダウンロード"](#)

["NetApp Interoperability Matrix Tool"](#)

Linuxホスト

- rootユーザまたはroot以外のユーザに対してパスワード ベースのSSH接続を有効にしておく必要があります。
- Java 11をLinuxホストにインストールしておく必要があります。

["すべてのオペレーティングシステム用のJAVAをダウンロード"](#)

"NetApp Interoperability Matrix Tool"

- LinuxホストでSAP HANAデータベースを実行している場合は、Plug-in for SAP HANA Databaseのインストール時にSnapCenter Plug-in for UNIXが自動的にインストールされます。
- プラグインのインストールには、デフォルトのシェルとして **bash** を使用する必要があります。

補助コマンド

SnapCenterプラグイン for SAP HANA で補足コマンドを実行するには、そのコマンドを *allowed_commands.config* ファイルに含める必要があります。

- Windows ホスト上のデフォルトの場所: *C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Linux ホスト上のデフォルトの場所: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

プラグイン ホストで補足コマンドを許可するには、エディターで *allowed_commands.config* ファイルを開きます。各コマンドを別々の行に入力します。コマンドでは大文字と小文字は区別されません。完全修飾パス名を指定し、パス名にスペースが含まれている場合は引用符 (") で囲んでください。

例えば：

command: mount

command: umount

コマンド: "C:\Program Files\ NetApp\ SnapCreator コマンド\sdcli.exe"

command: myscript.bat

allowed_commands.config ファイルが存在しない場合、コマンドまたはスクリプトの実行はブロックされ、ワークフローは次のエラーで失敗します。

"[/mnt/mount -a] の実行は許可されていません。Authorize by adding the command in the file %s on the plugin host."

コマンドまたはスクリプトが *allowed_commands.config* に存在しない場合、コマンドまたはスクリプトの実行はブロックされ、ワークフローは次のエラーで失敗します。

"[/mnt/mount -a] の実行は許可されていません。Authorize by adding the command in the file %s on the plugin host."



すべてのコマンドを許可するには、ワイルドカード エントリ (*) を使用しないでください。

Linuxホストのroot以外のユーザへのsudo権限の設定

SnapCenter 2.0以降のリリースでは、root以外のユーザがSnapCenter Plug-ins Package for Linuxをインストールしてプラグイン プロセスを開始できます。プラグイン プロセスは有効なroot以外のユーザとして実行されます。いくつかのパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

必要なもの

- sudoバージョン1.8.7以降

- umask が 0027 の場合、java フォルダーとその中のすべてのファイルに 555 の権限があることを確認します。そうしないと、プラグインのインストールが失敗する可能性があります。
- root以外のユーザについては、root以外のユーザの名前とユーザのグループが同じであることを確認してください。
- /etc/ssh/sshd_config ファイルを編集して、メッセージ認証コード アルゴリズム (MAC hmac-sha2-256 および MAC hmac-sha2-512) を設定します。

この構成ファイルを更新したら、sshdサービスを再起動します。

例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

このタスクについて

次のパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

- /home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /custom_location/NetApp/snapcenter/spl/bin/spl

手順

1. SnapCenter Plug-ins Package for LinuxをインストールするLinuxホストにログインします。
2. visudo Linuxユーティリティを使用して、/etc/sudoersファイルに次の行を追加します。

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Precchecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



RAC をセットアップしている場合は、他の許可されたコマンドとともに、`/etc/sudoers` ファイルに次の行を追加する必要があります: `'/<crs_home>/bin/olsnodes'`

`crs_home` の値は、`/etc/oracle/olr.loc` ファイルから取得できます。

`LINUX_USER` は、作成した非 root ユーザーの名前です。

`checksum_value` は、次の場所にある `sc_unix_plugins_checksum.txt` ファイルから取得できます。

- SnapCenter Server が Windows ホストにインストールされている場合は、`C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`。
- SnapCenter Server が Linux ホストにインストールされている場合は、`/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`。



この例は、独自のデータを作成する際の参照としてのみ使用してください。

SnapCenter Plug-ins Package for Windowsをインストールするホストの要件

SnapCenter Plug-ins Package for Windowsをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	Microsoft Windows サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	5 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	- ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル - PowerShell Core 7.4.2 - Java 11 Oracle Java および OpenJDK Java 11 Oracle Java および OpenJDK は、SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp対応プラグイン、および Windows ホストにインストールできるその他のカスタム アプリケーションにのみ必要です。 サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。

SnapCenter Plug-ins Package for Linuxをインストールするホストの要件

SnapCenter Plug-ins Package for Linuxをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	- Red Hat Enterprise Linux - SUSE Linux Enterprise Server (SLES) サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。

項目	要件
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	2 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエントリの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	Java 11 Oracle JavaおよびOpenJDK Javaを最新バージョンにアップグレードした場合は、<code>/var/opt/snapcenter/spl/etc/spl.properties</code>にある<code>JAVA_HOME</code>オプションが正しいJavaバージョンと正しいパスに設定されていることを確認する必要があります。 サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。

SnapCenter Plug-in for SAP HANA Databaseのクレデンシャルの設定

SnapCenterは、クレデンシャルを使用してSnapCenterの処理を実行するユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、データベースやWindowsファイルシステムでのデータ保護処理に使用するクレデンシャルをそれぞれ作成する必要があります。

タスク概要

- Linuxホスト

Linuxホストにプラグインをインストールするには、クレデンシャルを設定する必要があります。

このクレデンシャルは、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo権限があるroot以外のユーザに対して設定します。

ベスト プラクティス: ホストをデプロイしてプラグインをインストールした後も Linux の認証情報を作成できますが、ベスト プラクティスとしては、SVM を追加した後、ホストをデプロイしてプラグインをインストールする前に認証情報を作成します。

- Windowsホスト

プラグインのインストール前にWindowsクレデンシャルを設定する必要があります。

このクレデンシャルには、管理者権限（リモート ホストに対する管理者権限を含む）を設定する必要があります。

個々のリソース グループのクレデンシャルを設定する場合で、ユーザ名に完全なadmin権限が割り当てられていない場合は、少なくともリソース グループとバックアップの権限を割り当てる必要があります。

手順

- 1. 左側のナビゲーション ペインで、[設定] をクリックします。
- 2. [設定] ページで、[資格情報] をクリックします。
- 3. *新規* をクリックします。

Credential

Provide information for the Credential you want to add

Credential Name

Name

Username

Username

Password

Password

Authentication

Linux

☐ Use sudo privileges

Cancel

OK

- 4. [Credential] ページで、クレデンシャルの設定に必要な情報を指定します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。

フィールド	操作
ユーザ名	認証に使用するユーザ名とパスワードを入力します。 - ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者またはSnapCenterプラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。ユーザ名フィールドの有効な形式は次のとおりです。 ◦ <i>NetBIOS</i>\ユーザー名 ◦ ドメイン<i>FQDN</i>\ユーザー名 - ローカル管理者（ワークグループの場合のみ） ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。ユーザー名フィールドの有効な形式は次のとおりです: <i>UserName</i> パスワードには二重引用符 (") やバッククォート (') を使用しないでください。未満記号 (<) と感嘆符 (!) を組み合わせて使用したりしないでください。たとえば、lessthan<!10、lessthan10<!、バックティック `12 などです。
パスワード	認証に使用するパスワードを入力します。
Authentication Mode	使用する認証モードを選択します。
Use sudo privileges	非 root ユーザーの資格情報を作成する場合は、[sudo 権限を使用する] チェックボックスをオンにします。  Linuxユーザのみに該当します。

5. [OK]をクリックします。

クレデンシャルの設定が完了したら、必要に応じて[User and Access]ページでユーザやユーザ グループにクレデンシャルを割り当てることができます。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、作成したグループ管理サービス アカウント (gMSA) を通じて、管理対象ドメイン アカウントからサービス アカウントのパスワードを自動管理できます。

開始する前に

- Windows Server 2016以降のドメイン コントローラが必要です。
- ドメインのメンバーであるWindows Server 2016以降のホストが必要です。

手順

1. KDSルート キーを作成し、gMSA内のオブジェクトごとに一意のパスワードを生成します。
2. 各ドメインについて、Windowsドメインコントローラから次のコマンドを実行します: Add-KDSRootKey -EffectiveImmediately
3. gMSAを作成して設定します。
 - a. 次の形式でユーザ グループ アカウントを作成します。

```
domainName\accountName$  
.. コンピュータ オブジェクトをグループに追加します。  
.. 作成したユーザ グループを使用してgMSAを作成します。
```

次に例を示します。

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 走る `Get-ADServiceAccount` サービス アカウントを確認するコマンド。
```

4. ホストでgMSAを設定します。
 - a. gMSAアカウントを使用するホストで、Windows PowerShell用のActive Directoryモジュールを有効にします。

これを行うには、PowerShellから次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. ホストを再起動します。
- b. PowerShell コマンド プロンプトから次のコマンドを実行して、ホストに gMSA をインストールします。 `Install-AdServiceAccount <gMSA>`
- c. 次のコマンドを実行して、gMSA アカウントを確認します。 `Test-AdServiceAccount <gMSA>`
5. ホスト上の設定済みgMSAに管理者権限を割り当てます。
6. SnapCenter Serverで設定済みのgMSAアカウントを指定してWindowsホストを追加します。

SnapCenter Serverにより、選択したプラグインがホストにインストールされ、プラグインのインストール時には指定したgMSAがサービスのログオン アカウントとして使用されます。

SnapCenter Plug-in for SAP HANA Databaseのインストール

ホストの追加とリモート ホストへのプラグイン パッケージのインストール

SnapCenterの[Add Host]ページを使用してホストを追加し、プラグイン パッケージをインストールする必要があります。プラグインは、自動的にリモート ホストにインストールされます。ホストの追加とプラグイン パッケージのインストールは、ホストごとまたはクラスタごとに行うことができます。

開始する前に

- SnapCenter Serverホストのオペレーティング システムがWindows 2019で、プラグイン ホストのオペレーティング システムがWindows 2022の場合は、次の手順を実行する必要があります。
 - Windows Server 2019 (OSビルド17763.5936) 以降にアップグレードする
 - Windows Server 2022 (OSビルド20348.2402) 以降にアップグレードする
- この処理は、SnapCenter Adminロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。

- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカルワークグループに属している場合は、ホストのUACを無効にする必要があります。
- メッセージキューサービスが実行中であることを確認する必要があります。
- ホストの管理については、管理に関するドキュメントを参照してください。
- グループ管理サービスアカウント（gMSA）を使用する場合は、管理者権限でgMSAを設定する必要があります。

"Windows Server 2016 以降で SAP HANA 用のグループ管理サービス アカウントを構成する"

タスク概要

- SnapCenter Serverをプラグイン ホストとして別のSnapCenter Serverに追加することはできません。
- SAP HANA システムレプリケーションがプライマリシステムとセカンダリシステムの両方のリソースを検出するには、root または sudo ユーザーを使用してプライマリシステムとセカンダリシステムの両方を追加することをお勧めします。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. 上部の*管理対象ホスト*タブが選択されていることを確認します。
3. *[追加]*をクリックします。
4. [Hosts]ページで、次の操作を実行します。

フィールド	操作
ホストタイプ	ホストのタイプを選択します。 • Windows • Linux  Plug-in for SAP HANA は、HDBSQLクライアント ホストにインストールされます。このホストは、WindowsシステムでもLinuxシステムでもかまいません。
ホスト名	通信ホスト名を入力します。ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。SnapCenterが機能するためには、DNSが適切に設定されている必要があります。そのため、FQDNを入力することを推奨します。 HDBSQLクライアントとHDBUserStoreをこのホスト上に設定する必要があります。

フィールド	操作
Credentials	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。このクレデンシャルには、リモート ホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。  クレデンシャルの認証モードは、[Add Host]ウィザードで指定するホスト タイプによって決まります。

5. [Select Plug-ins to Install]セクションで、インストールするプラグインを選択します。

6. (オプション) [その他のオプション] をクリックします。

フィールド	操作
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。デフォルトのポート番号は8145です。SnapCenter Serverがカスタム ポートにインストールされている場合は、そのポート番号がデフォルト ポートとして表示されます。  プラグインを手動でインストールしてカスタム ポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理が失敗します。
Installation Path	Plug-in for SAP HANAは、HDBSQLクライアントホストにインストールされます。このホストは、WindowsシステムでもLinuxシステムでもかまいません。 - Windows 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは C:\Program Files\ NetApp\ SnapCenterです。必要に応じて、パスをカスタマイズできます。 - Linux 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは /opt/ NetApp/snapcenter です。必要に応じて、パスをカスタマイズできます。

フィールド	操作
Skip preinstall checks	プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスをオンにします。
Use group Managed Service Account (gMSA) to run the plug-in services	Windowsホストで、グループ管理サービス アカウント (gMSA) を使用してプラグイン サービスを実行する場合は、このチェック ボックスをオンにします。  gMSA名 をdomainName\accountName\$の形式で指定します。  gMSAは、SnapCenter Plug-in for Windowsサービスのログオン サービス アカウントとしてのみ使用されます。

7. *送信*をクリックします。

[Skip prechecks]チェック ボックスを選択していない場合、プラグインをインストールするための要件をホストが満たしているかどうかを検証するためにホストが検証されます。ディスク スペース、RAM、PowerShellのバージョン、.NETのバージョン、場所（Windowsプラグインの場合）、Javaのバージョン（Linuxプラグインの場合）が最小要件に照らして検証されます。最小要件を満たしていない場合、対応するエラーまたは警告メッセージが表示されます。

エラーがディスク スペースまたはRAMに関連している場合は、C:\Program Files\NetApp\SnapCenter WebAppにあるweb.configファイルを更新してデフォルト値を変更できます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。



HAのセットアップでweb.configファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. ホスト タイプが Linux の場合は、フィンガープリントを確認し、[確認して送信] をクリックします。

クラスタ セットアップでは、クラスタ内の各ノードのフィンガープリントを検証する必要があります。



前述の手順で同じホストがSnapCenterに追加され、フィンガープリントが確認された場合でも、フィンガープリントの検証は必須です。

9. インストールの進捗状況を監視します。

インストール固有のログ ファイルは、/custom_location/snapcenter/logsにあります。

コマンドレットを使用した複数のリモート ホストへの**SnapCenter Plug-ins Package for Linux / Windows**のインストール

Install-SmHostPackage PowerShellコマンドレットを使用すると、複数のホストにSnapCenter Plug-ins Package for Linux / Windowsを同時にインストールできます。

開始する前に

プラグイン パッケージをインストールする各ホストに対するローカル管理者権限を持つドメイン ユーザとして、SnapCenterにログインしておく必要があります。

手順

1. PowerShellを起動します。
2. SnapCenter Serverホストで、Open-SmConnectionコマンドレットを使用してセッションを確立し、クレデンシャルを入力します。
3. Install-SmHostPackageコマンドレットと必要なパラメータを使用して、複数のホストにプラグインをインストールします。

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、-skipprecheckオプションを使用できます。

4. リモート インストールのクレデンシャルを入力します。

コマンドライン インターフェイスを使用した**Linux**ホストへの**SnapCenter Plug-in for SAP HANA Database**のインストール

SnapCenter Plug-in for SAP HANA Databaseは、SnapCenterユーザ インターフェイス (UI) を使用してインストールする必要があります。SnapCenter UIからのプラグインのリモート インストールが許可されていない環境では、コマンドライン インターフェイス (CLI) を使用して、コンソール モードまたはサイレント モードでPlug-in for SAP HANA Databaseをインストールできます。

開始する前に

- Plug-in for SAP HANA Databaseは、HDBSQLクライアントがあるLinuxホストごとにインストールする必要があります。
- SnapCenter Plug-in for SAP HANA DatabaseをインストールするLinuxホストは、依存するソフトウェア、データベース、オペレーティング システムの要件を満たしている必要があります。

サポートされる構成に関する最新の情報については、Interoperability Matrix Tool (IMT) を参照してください。

<https://imt.netapp.com/matrix/imt.jsp?components=121029;&solution=1259&isHWU&src=IMT>

- SnapCenter Plug-in for SAP HANA Databaseは、SnapCenter Plug-ins Package for Linuxに含まれています。SnapCenter Plug-ins Package for Linuxをインストールする前に、SnapCenterをWindowsホストにインストールしておく必要があります。

手順

1. SnapCenter Plug-ins Package for Linuxのインストール ファイル (snapcenter_linux_host_plugin.bin) をC:\ProgramData\NetApp\SnapCenter\Package RepositoryからPlug-in for SAP HANA Databaseをインストールするホストにコピーします。

このパスには、SnapCenter Serverがインストールされているホストからアクセスできます。

2. コマンド プロンプトから、インストール ファイルをコピーしたディレクトリに移動します。
3. プラグインをインストールします。

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address  
-DSERVER_HTTPS_PORT=port_number_for_server
```

- -DPORT は SMCORE HTTPS 通信ポートを指定します。
- -DSERVER_IP は、 SnapCenter Server の IP アドレスを指定します。
- -DSERVER_HTTPS_PORT は、 SnapCenter Server の HTTPS ポートを指定します。
- -DUSER_INSTALL_DIR は、Linux 用のSnapCenterプラグイン パッケージをインストールするディレクトリを指定します。
- DINSTALL_LOG_NAME はログ ファイルの名前を指定します。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146  
-DUSER_INSTALL_DIR=/opt  
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log  
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. /<インストール ディレクトリ>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties ファイルを編集し、PLUGINS_ENABLED = hana:3.0 パラメータを追加します。
5. Add-Smhostコマンドレットと必要なパラメータを使用して、SnapCenter Serverにホストを追加します。

コマンドで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

Plug-in for SAP HANAのインストール ステータスの監視

[Jobs]ページを使用して、SnapCenterプラグイン パッケージのインストールの進捗状況を監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました

-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、プラグインのインストール操作のみがリストされるようにリストをフィルタリングするには、次の手順を実行します。
 - a. *フィルター*をクリックします。
 - b. オプション：開始日と終了日を指定します。
 - c. [タイプ] ドロップダウン メニューから、[プラグインのインストール] を選択します。
 - d. [Status]ドロップダウン メニューから、インストールのステータスを選択します。
 - e. *適用*をクリックします。
4. インストール ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

CA証明書の設定

CA証明書CSRファイルの生成

証明書署名要求（CSR）を生成し、生成したCSRを使用して認証局（CA）から取得した証明書をインポートできます。証明書には秘密キーが関連付けられます。

CSRはエンコードされたテキストのブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。



CA 証明書の RSA キーの長さは最低 3072 ビットである必要があります。

CSRを生成するための情報については、["CA証明書CSRファイルの生成方法"](#)。



ドメイン (*.domain.company.com) またはシステム (machine1.domain.company.com) の CA 証明書を所有している場合は、CA 証明書 CSR ファイルの生成をスキップできます。SnapCenterを使用して、既存のCA証明書を導入できます。

クラスタ構成の場合、クラスタ名（仮想クラスタFQDN）と、それぞれのホスト名がCA証明書に記載されている必要があります。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。ワイルドカード証明書 (*.domain.company.com) の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenter ServerとWindowsホスト プ

ログインにCA証明書をインポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
4. コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書 をクリックします。
5. 「信頼されたルート証明機関」フォルダを右クリックし、[すべてのタスク] > [インポート] を選択して、インポート ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*次へ*をクリックします。
インポート ファイル形式	変更せずに、[次へ] をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、[次へ] をクリックします。
証明書のインポート ウィザードの完了	概要を確認し、[完了] をクリックしてインポートを開始します。



インポートする証明書は秘密キーとバンドルされている必要があります (サポートされている形式は **.pfx**、**.p12**、および ***.p7b** です)。

7. 「個人用」フォルダに対して手順5を繰り返します。

CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための16進数の文字列です。サムプリントは、サムプリント アルゴリズムを使用して証明書の内容から計算されます。

手順

1. GUIで次の手順を実行します。
 - a. 証明書をダブルクリックします。
 - b. [証明書] ダイアログボックスで、[詳細] タブをクリックします。
 - c. フィールドのリストをスクロールして、「拇印」をクリックします。
 - d. ボックスから16進数の文字をコピーします。

- e. 16進数の間のスペースを削除します。

たとえば、拇印が「a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b」の場合、スペースを削除すると「a909502dd82ae41433e6f83886b00d4277a32a7b」になります。

- 2. PowerShellで、次の手順を実行します。

- a. 次のコマンドを実行して、インストールされている証明書のサムプリントを表示し、最近インストールされた証明書をサブジェクト名で識別します。

```
Get-ChildItem -Path 証明書:\LocalMachine\My
```

- b. サムプリントをコピーします。

Windowsホスト プラグイン サービスでのCA証明書の設定

インストールされているデジタル証明書をアクティブ化するには、Windowsホスト プラグイン サービスを使用してCA証明書を設定する必要があります。

SnapCenter Serverと、CA証明書がすでに導入されているすべてのプラグイン ホストで、次の手順を実行します。

手順

- 1. 次のコマンドを実行して、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例えば：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

． 次のコマンドを実行して、新しくインストールした証明書をWindowsホスト プラグイン サービスとバインドします。

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

例えば：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

LinuxホストでのSnapCenter SAP HANAプラグイン サービスのCA証明書の設定

インストールされたデジタル証明書をアクティブ化するには、SnapCenterプラグインサービスを使用して、プラグイン キーストアとその証明書のパスワードを管理し、CA証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、`/opt/NetApp/snapcenter/scc/etc`にあるファイル「`keystore.jks`」を使用します。

プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

キー「`KEYSTORE_PASS`」に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```

・ キーストア内の秘密キー
エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

`agent.properties` ファイルのキー `KEYSTORE_PASS` も同様に更新します。

3. パスワードを変更したら、サービスを再起動します。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは同じである必要があります。

ルート証明書または中間証明書をプラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグイン キーストアが含まれるフォルダーに移動します: `/opt/NetApp/snapcenter/scc/etc`。
2. 「`keystore.jks`」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. ルート証明書か中間証明書を追加します。

```
keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

・ ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアにCA署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグイン キーストア /opt/ NetApp/snapcenter/scc/etc が含まれるフォルダーに移動します。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

6. キーストアに追加された新しいCA証明書に対応するエイリアスが、キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのプラグイン キーストア パスワードは、agent.properties ファイルのキー KEYSTORE_PASS の値です。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
```

・ CA 証明書のエイリアス名が長く、スペースや特殊文字（「*」、「」）が含まれている場合は、エイリアス名を単純な名前に変更します。

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
```

・ agent.properties ファイルのCA証明書からエイリアス名を設定します。

この値を、キーSCC_CERTIFICATE_ALIASに対して更新します。

8. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

プラグインの証明書失効リスト (CRL) を構成する

タスク概要

- SnapCenterプラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- SnapCenterプラグインの CRL ファイルのデフォルト ディレクトリは、「opt/NetApp/snapcenter/scc/etc/crl」です。

手順

1. キーCRL_PATHに対して、agent.propertiesファイルのデフォルト ディレクトリを変更、更新できます。

このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

WindowsホストでのSnapCenter SAP HANAプラグインサービスのCA証明書の設定

インストールされたデジタル証明書をアクティブ化するには、SnapCenterプラグインサービスを使用して、プラグイン キーストアとその証明書のパスワードを管理し、CA証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etcにあるファイル *keystore.jks* を使用します。

プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

これはキー_KEYSTORE_PASS_に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```



Windowsコマンド プロンプトで「keytool」 コマンドが認識されない場合は、keytoolコマンドを完全なパスに置き換えます。

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. キーストア内の秘密キー エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

```
keytool -keypasswd -alias "証明書内のエイリアス名" -keystore keystore.jks
```

agent.properties ファイルのキー KEYSTORE_PASS も同様に更新します。

4. パスワードを変更したら、サービスを再起動します。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは同じである必要があります。

ルート証明書または中間証明書をプラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_` に移動します。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. ルート証明書か中間証明書を追加します。

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアにCA署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_` に移動します。
2. ファイル `keystore.jks` を見つけます。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

6. キーストアに追加された新しいCA証明書に対応するエイリアスが、キーストアに含まれていることを確認します。

7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのプラグイン キーストア パスワードは、`agent.properties` ファイルのキー `KEYSTORE_PASS` の値です。

```
keytool -keypasswd -alias "CA証明書のエイリアス名" -keystore keystore.jks
```

8. `agent.properties` ファイル内の CA 証明書からエイリアス名を設定します。

この値を、キー `SCC_CERTIFICATE_ALIAS` に対して更新します。

9. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

SnapCenterプラグインの証明書失効リスト（CRL）を構成する

タスク概要

- 関連するCA証明書の最新のCRLファイルをダウンロードするには、"[SnapCenter CA証明書の証明書失効リストファイルを更新する方法](#)"。
- SnapCenterプラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- SnapCenterプラグインの CRL ファイルのデフォルト ディレクトリは、'`C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\ etc\crl`' です。

手順

1. キー `CRL_PATH` に対して、`agent.properties` ファイル内のデフォルト ディレクトリを変更および更新できます。
2. このディレクトリには、複数のCRLファイルを格納できます。

受信する証明書については、それぞれのCRLに対して検証が行われます。

プラグインのCA証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインでCA証明書の検証を有効にする必要があります。

開始する前に

- 実行 `Set-SmCertificateSettings` コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- `Get-SmCertificateSettings` を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. プラグイン ホストを1つまたは複数選択します。
4. *その他のオプション*をクリックします。

5. *証明書の検証を有効にする*を選択します。

終了後の操作

[Managed Hosts]タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Serverとプラグイン ホスト間の接続のステータスを示します。

- *  * は、CA 証明書が有効になっていないか、プラグイン ホストに割り当てられていないことを示します。
- *  * は CA 証明書が正常に検証されたことを示します。
- *  * は、CA 証明書を検証できなかったことを示します。
- *  * は接続情報を取得できなかったことを示します。



ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

SnapCenter Plug-in for VMware vSphereのインストール

データベースまたはファイルシステムが仮想マシン（VM）に格納されている場合や、VMとデータストアを保護する場合は、SnapCenter Plug-in for VMware vSphere仮想アプライアンスを導入する必要があります。

展開方法については、["導入プロセスの概要"](#)。

CA証明書を導入する

SnapCenter Plug-in for VMware vSphereで CA 証明書を構成するには、以下を参照してください。 ["SSL証明書を作成またはインポートする"](#)。

CRLファイルを設定する

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリでCRLファイルを探します。SnapCenter Plug-in for VMware vSphere のCRL ファイルのデフォルト ディレクトリは `/opt/netapp/config/crl` です。

このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

データ保護の準備

SnapCenter Plug-in for SAP HANA Databaseを使用するための前提条件

ユーザがSnapCenter Plug-in for SAP HANA Databaseを使用するためには、SnapCenter管理者が事前にSnapCenter Serverをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter Serverをインストールして設定します。

- SnapCenter Serverにログインします。
- SnapCenter環境を設定するために、必要に応じて、ストレージ システム接続を追加し、クレデンシャルを作成します。
- LinuxホストまたはWindowsホストにJava 11をインストールします。

Javaパスは、ホスト マシンの環境パス変数で設定する必要があります。

- バックアップ レプリケーションが必要である場合は、SnapMirrorとSnapVaultをセットアップします。
- Plug-in for SAP HANA DatabaseをインストールするホストにHDBSQLクライアントをインストールします。

このホストで管理するSAP HANAノードのユーザ ストア キーを設定します。

- SAP HANAデータベース2.0SPS05でSAP HANAデータベース ユーザ アカウントを使用している場合は、SnapCenter Serverでバックアップ、リストア、クローニングの処理を実行するための次の権限があることを確認してください。
 - バックアップ管理者
 - カタログ読み取り
 - データベース バックアップ管理者
 - データベース リカバリ運用者

SAP HANAデータベースの保護におけるリソース、リソース グループ、ポリシーの使用 方法

SnapCenterを使用する前に、実行するバックアップ、クローニング、リストアの各処理に関連する基本的な概念を理解しておく役立ちます。ここでは、これらの処理で扱うリソース、リソース グループ、およびポリシーについて説明します。

- リソースとは、一般にはSnapCenterでバックアップまたはクローニングするSAP HANAデータベースのことです。
- SnapCenterリソース グループは、ホスト上のリソースの集まりです。

リソース グループに対して処理を実行すると、リソース グループに指定したスケジュールに従って、リソース グループに定義されているリソースに対して処理が実行されます。

単一のリソースまたはリソース グループをオンデマンドでバックアップすることができます。また、スケジュールされたバックアップを単一リソースおよびリソース グループに対して実行することもできます。

- ポリシーは、バックアップ頻度、レプリケーション、スクリプトといった、データ保護処理の特性を指定するものです。

リソース グループを作成するときに、そのグループに対して1つ以上のポリシーを選択します。単一リソースに対してオンデマンドでバックアップを実行するときにもポリシーを選択できます。

リソース グループでは、保護する対象と保護するタイミング（日時）を定義できます。ポリシーでは、保護する方法を定義できます。たとえば、すべてのデータベースをバックアップする場合は、ホストのすべてのデータベースを含むリソース グループを作成します。このリソース グループに、日次ポリシーと毎時ポリシー

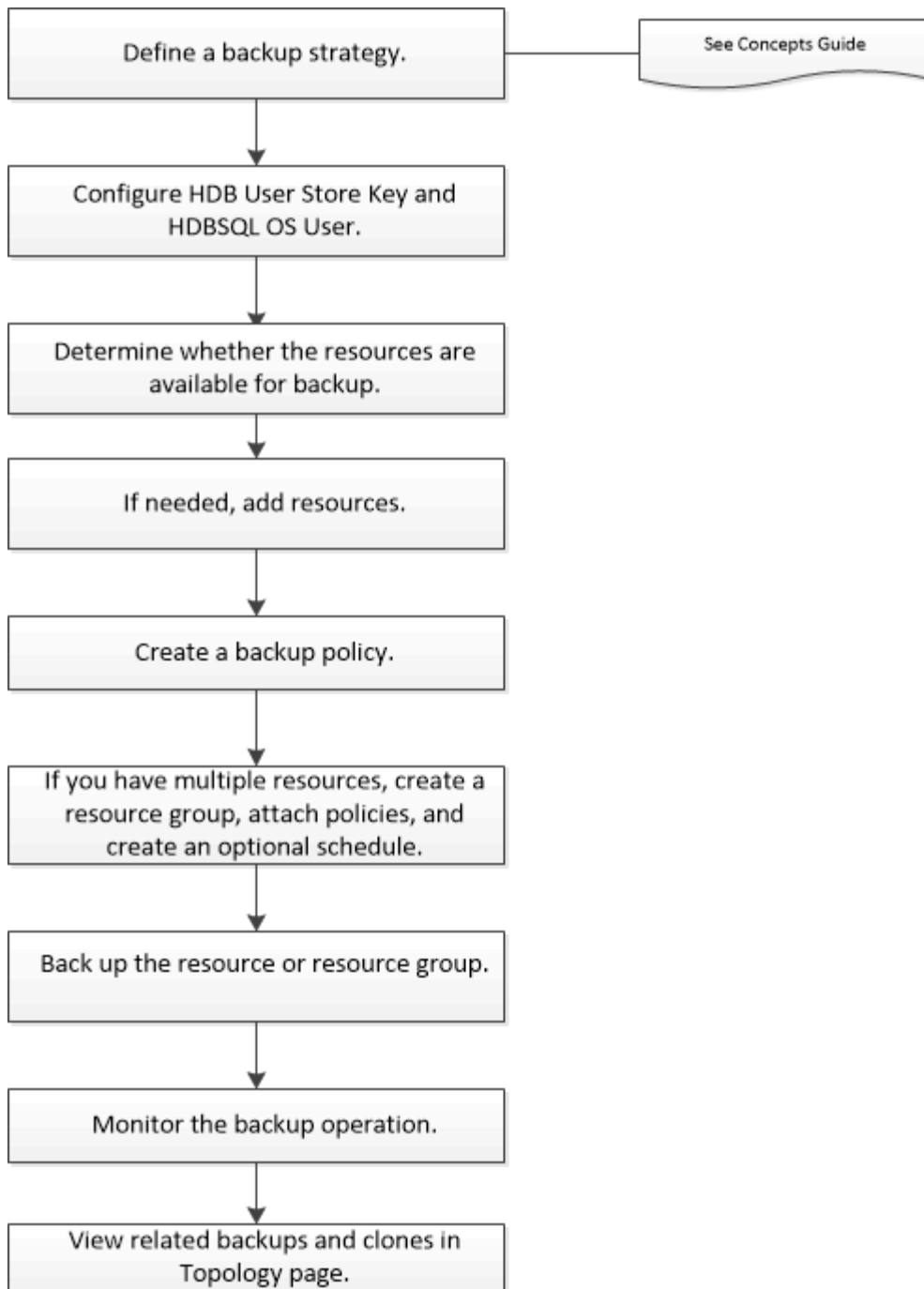
の2つのポリシーを適用します。リソース グループを作成してポリシーを適用する際に、フル バックアップを1日1回実行するようにリソース グループを設定できます。

SAP HANAリソースのバックアップ

SAP HANAリソースのバックアップ

リソース（データベース）またはリソース グループのバックアップを作成することができます。バックアップのワークフローには、計画、バックアップするデータベースの特定、バックアップ ポリシーの管理、リソース グループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

次のワークフローは、バックアップ処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。<https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html>["SnapCenterソフトウェア コマンドレット リファレンス ガイド"]。

SAP HANAデータベースのHDBユーザ ストア キーとHDBSQL OSユーザの設定

SAP HANAデータベースでデータ保護処理を実行するには、HDBユーザ ストア キーとHDBSQL OSユーザを設定する必要があります。

開始する前に

- SAP HANAデータベースにHDBのセキュアなユーザ ストア キーとHDB SQL OSユーザが設定されていない場合は、自動検出されたリソースに対してのみ赤い南京錠アイコンが表示されます。以降の検出処理中に、設定済みのHDBのセキュアなユーザ ストア キーが正しくないか、データベース自体へのアクセスが提供されていないと判断された場合は、赤い南京錠アイコンが再表示されます。
- データベースを保護できるようにHDBのセキュアなユーザ ストア キーとHDB SQL OSユーザを設定するか、またはデータベースをリソース グループに追加してデータ保護処理を実行する必要があります。
- システム データベースにアクセスするようにHDB SQL OSユーザを設定する必要があります。テナント データベースにのみアクセスするようにHDB SQL OSユーザが設定されている場合、検出処理は失敗します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから[SnapCenter Plug-in for SAP HANA Database] を選択します。
2. [リソース] ページで、[表示] リストからリソース タイプを選択します。
3. (オプション) クリック  ホスト名を選択します。

そのあとに  をクリックすると、フィルタ ペインが閉じます。

4. データベースを選択し、「データベースの構成」をクリックします。
5. [Configure database settings]セクションで、「HDB Secure User Store Key」と入力します。



プラグインのホスト名が表示され、HDB SQL OS ユーザーは <sid>adm に自動的に入力されます。

6. [OK]をクリックします。

[Topology]ページでデータベース設定を変更できます。

データ保護のためのリソースの検出とマルチテナント データベース コンテナの準備

データベースの自動的検出

リソースとは、SnapCenterで管理するLinuxホスト上のSAP HANAデータベースとデータ ボリューム以外のボリュームです。使用できるSAP HANAデータベースを検出したあとに、これらのリソースをリソース グループに追加してデータ保護処理を実行できます。

開始する前に

- SnapCenter Serverのインストール、HDBユーザ ストア キーの追加、ホストの追加、ストレージ システム接続のセットアップなどのタスクを完了しておく必要があります。
- LinuxホストでHDBのセキュアなユーザ ストア キーとHDB SQL OSユーザを設定しておく必要があります。
 - SID admユーザを使用してHDBユーザ ストア キーを設定する必要があります。たとえば、SIDとしてA22を使用するHANAシステムの場合は、HDBユーザ ストア キーをa22admに設定します。
- SnapCenter Plug-in for SAP HANA Databaseでは、RDM / VMDK仮想環境にあるリソースの自動検出がサポートされていません。データベースを手動で追加する際に、仮想環境のストレージの情報を指定する必要があります。

タスク概要

プラグインをインストールすると、そのLinuxホスト上のすべてのリソースが自動検出されて[Resources]ページに表示されます。

自動検出されたリソースを変更または削除することはできません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから SAP HANA データベース用プラグインを選択します。
2. [Resources] ページで、[View] リストからリソース タイプを選択します。
3. (オプション) をクリック 、ホスト名を選択します。

をクリックします  フィルター パネルを閉じます。

4. ホスト上で利用可能なリソースを検出するには、[リソースの更新] をクリックします。

リソースは、リソース タイプ、ホスト名、関連するリソース グループ、バックアップ タイプ、ポリシー、全体的なステータスなどの情報とともに表示されます。

- データベースがNetAppストレージにあって保護されていない場合は、[Overall Status]列に「Not protected」と表示されます。
- データベースがNetAppストレージ システム上にあって保護されており、バックアップ処理が実行されていない場合は、[Overall Status]列に「Backup not run is displayed」と表示されます。それ以外の場合は、前回のバックアップ ステータスに基づいて、ステータスが「バックアップに失敗しました」または「バックアップに成功しました」に変わります。



SAP HANAデータベースでHDBのセキュアなユーザ ストア キーが設定されていない場合は、リソースの横に赤い南京錠アイコンが表示されます。以降の検出処理中に、設定済みのHDBのセキュアなユーザ ストア キーが正しくないか、データベース自体へのアクセスが提供されていないと判断された場合は、赤い南京錠アイコンが再表示されます。



SnapCenterの外部でデータベースの名前が変更された場合は、リソースを更新する必要があります。

終了後の操作

データベースを保護できるようにHDBのセキュアなユーザ ストア キーとHDBSQL OSユーザを設定するか、またはデータベースをリソース グループに追加してデータ保護処理を実行する必要があります。

"SAP HANAデータベースのHDBユーザ ストア キーとHDBSQL OSユーザの設定"

データ保護のためのマルチテナント データベース コンテナの準備

SnapCenterに直接登録されているSAP HANAホストの場合、SnapCenter Plug-in for SAP HANA Databaseをインストールまたはアップグレードすると、ホスト上のリソースの自動検出がトリガーされます。プラグインのインストールまたはアップグレード後には、プラグイン ホストに配置されていたマルチテナント データベース コンテナ (MDC) リソースそれぞれが、異なるGUID形式を持つ別のMDCリソースとして自動的に検出され、SnapCenterに登録されます。新しいリソースは「ロックされた」状態になります。

す。

タスク概要

たとえば、SnapCenter 4.2で、E90 MDCリソースがプラグイン ホストにあり、手動で登録されていた場合、SnapCenter 4.3へのアップグレード後には、異なるGUIDを持つ別のE90 MDCリソースが検出されてSnapCenterに登録されます。



SnapCenter 4.2以前のバージョンのリソースに関連するバックアップは、保持期間が終了するまで保持する必要があります。保持期間が終了したら、古いMDCリソースは削除してかまいません。自動検出された新しいMDCリソースで管理を続行できます。

`Old MDC resource` SnapCenter 4.2 以前のリリースで手動で追加されたプラグイン ホストの MDC リソースです。

SnapCenter 4.3で検出された新しいリソースを使用してデータ保護処理を行うには、次の手順を実行します。

手順

1. [リソース] ページで、以前のSnapCenterリリースにバックアップが追加された古い MDC リソースを選択し、[トポロジ] ページからそれを「メンテナンス モード」に設定します。

リソースがリソース グループの一部である場合は、リソース グループを「メンテナンス モード」にします。

2. SnapCenter 4.3へのアップグレード後に検出された新しいMDCリソースを[Resources]ページで選択し、構成します。

「新しい MDC リソース」は、SnapCenterサーバとプラグイン ホストが 4.3 にアップグレードされた後に新しく検出された MDC リソースです。そのホストでの古いMDCリソースと同じSIDを持つリソースが新しいMDCリソースです。[Resources]ページでは、横に赤い南京錠のアイコンが表示されます。

3. 保護ポリシー、スケジュール、および通知設定を選択して、SnapCenter 4.3へのアップグレード後に検出された新しいMDCリソースを保護します。
4. 保持設定に基づいて、SnapCenter 4.2以前のリリースで作成されたバックアップを削除します。
5. [Topology]ページからリソース グループを削除します。
6. [Resources]ページから古いMDCリソースを削除します。

たとえば、プライマリ スナップショットの保持期間が 7 日間で、セカンダリ スナップショットの保持期間が 45 日間の場合、45 日が経過し、すべてのバックアップが削除された後に、リソース グループと古い MDC リソースを削除する必要があります。

関連情報

["SAP HANAデータベースのHDBユーザ ストア キーとHDBSQL OSユーザの設定"](#)

["\[Topology\]ページでのSAP HANAデータベースのバックアップとクローンの表示"](#)

手動でのプラグイン ホストへのリソースの追加

特定のHANAインスタンスでは、自動検出がサポートされていません。このようなリソースは手動で追加する必要があります。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続のセットアップ、HDBユーザ ストア キーの追加などのタスクを完了しておく必要があります。
- SAP HANAシステム レプリケーションでは、そのHANAシステムのすべてのリソースを1つのリソース グループに追加し、リソース グループのバックアップを作成することを推奨します。これにより、テイクオーバー / フェイルバック モードでのシームレスなバックアップが保証されます。

"リソース グループの作成とポリシーの適用"。

タスク概要

自動検出は、次の構成ではサポートされていません。

- RDMおよびVMDKレイアウト



上記のリソースが検出された場合、これらのリソースではデータ保護処理がサポートされません。

- HANAマルチホスト構成
- 同じホスト上の複数のインスタンス
- マルチティア スケールアウトHANAシステム レプリケーション
- システム レプリケーション モードのカスケード レプリケーション環境

手順

1. 左側のナビゲーション ペインで、ドロップダウン リストから SAP HANA データベース用のSnapCenter プラグインを選択し、リソース をクリックします。
2. リソース ページで、**SAP HANA** データベースの追加 をクリックします。
3. [Provide Resource Details]ページで、次の操作を実行します。

フィールド	操作
リソース タイプ	リソース タイプを入力します。リソース タイプは、単一のコンテナ、マルチテナント データベース コンテナ (MDC) 、データ ボリューム以外のボリュームです。
HANA システム名	SAP HANAシステムのわかりやすい名前を入力します。このオプションは、単一のコンテナまたはMDCリソース タイプを選択した場合にのみ使用できます。
SID	システムID (SID) を入力します。インストールされたSAP HANAシステムは単一のSIDで識別されます。
プラグイン ホスト	プラグイン ホストを選択します。

フィールド	操作
HDB のセキュアなユーザ ストア キー	SAP HANAシステムに接続するためのキーを入力します。 このキーには、データベースに接続するためのログイン情報が含まれます。 SAP HANAシステム レプリケーションでは、セカンダリ ユーザ キーは検証されません。これは、テイクオーバー時に使用されます。
HDBSQL OS ユーザ	HDB セキュア ユーザー ストア キーが設定されているユーザー名を入力します。Windows の場合、HDBSQL OS ユーザーは SYSTEM ユーザーである必要があります。したがって、SYSTEM ユーザーに対して HDB セキュア ユーザー ストア キーを構成する必要があります。

4. [ストレージ フットプリントの提供] ページで、ストレージ システムを選択し、1 つ以上のボリューム、LUN、および qtrees を選択して、[保存] をクリックします。

オプション：をクリックすることもできます  アイコンをクリックして、他のストレージ システムからボリューム、LUN、qtrees を追加します。

5. 概要を確認し、[完了] をクリックします。

データベースは、SID、プラグイン ホスト、関連するリソース グループとポリシー、全体的なステータスなどの情報とともに表示されます。

リソースへのアクセスをユーザに許可する場合は、ユーザにリソースを割り当てる必要があります。これにより、ユーザは、自身に割り当てられたアセットに対して、権限のある処理を実行できるようになります。

"ユーザまたはグループの追加と、ロールとアセットの割り当て"

データベースの追加が完了したら、SAP HANAデータベースの詳細を変更できます。

SAP HANAリソースに関連付けられているバックアップがある場合、次の項目は変更できません。

- マルチテナントデータベースコンテナ (MDC) : SIDまたはHDBSQLクライアント (プラグイン) ホスト
- 単一コンテナ: SID または HDBSQL クライアント (プラグイン) ホスト
- 非データボリューム: リソース名、関連SID、またはプラグインホスト

SAP HANAデータベースのバックアップ ポリシーの作成

SnapCenterを使用してSAP HANAデータベースのリソースをバックアップする前に、バックアップ対象のリソースまたはリソース グループのバックアップ ポリシーを作成する必要があります。バックアップ ポリシーとは、バックアップをどのように管理し、スケ

ジャーリングし、保持するかを定める一連のルールです。

開始する前に

- バックアップ戦略を定義しておく必要があります。

詳細については、SAP HANAデータベースのデータ保護戦略の定義に関する情報を参照してください。

- SnapCenterのインストール、ホストの追加、ストレージ システム接続の作成、リソースの追加などのタスクを実行して、データ保護の準備をしておく必要があります。
- ユーザがSnapshotをミラーまたはバックアップにレプリケートする場合は、ソース ボリュームとデスティネーション ボリューム両方のSVMをSnapCenter管理者がユーザに割り当てる必要があります。

ポリシーで、レプリケーション、スクリプト、アプリケーション設定を指定することもできます。それらのオプションを指定しておくことで、別のリソース グループにポリシーを再利用して時間を節約することができます。

- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、["SnapMirrorアクティブ同期のオブジェクト数の制限"](#)。

タスク概要

- SAP HANAシステム レプリケーション

- プライマリSAP HANAシステムの保護では、すべてのデータ保護処理を実行できます。
- セカンダリSAP HANAシステムの保護では、バックアップを作成することはできません。

フェイルオーバー後は、セカンダリSAP HANAシステムがプライマリSAP HANAシステムになるため、すべてのデータ保護処理を実行できます。

SAP HANAデータ ボリュームのバックアップを作成することはできませんが、SnapCenterはデータ以外のボリューム（NDV）の保護を継続します。

- SnapLock

- [Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで指定した保持日数以下にする必要があります。
- Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、ポリシーで指定した数よりも多くのSnapshotが保持される可能性があります。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[ポリシー]をクリックします。
3. *新規*をクリックします。
4. 「名前」 ページで、ポリシー名と詳細を入力します。
5. ポリシー タイプ ページで、次の手順を実行します。
 - ストレージタイプを選択

- 。バックアップ タイプを選択します。

状況	操作
Snapshotテクノロジーを使用してバックアップを作成する	*スナップショットベース*を選択します。
データベースの整合性チェックを実行する	*ファイルベースのバックアップ*を選択します。アクティブなテナントのみがバックアップされます。

6. スナップショットとレプリケーション ページで、次の手順を実行します。

- 。オンデマンド、時間別、日次、週次、または*月次*を選択してスケジュール タイプを指定します。



リソース グループを作成する際に、バックアップ処理のスケジュール（開始日、終了日、頻度）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソース グループを作成できますが、各ポリシーに異なるバックアップ スケジュールを割り当てることもできます。



午前 2 時にスケジュールを設定した場合、夏時間 (DST) 中はスケジュールは実行されません。

7. [スナップショットとレプリケーション] ページで、[バックアップ タイプ] ページで選択したバックアップ タイプとスケジュール タイプの保持設定を指定します。

状況	操作
特定の数のSnapshotを保持	*保持するコピー*を選択し、保持するスナップショットの数を指定します。 スナップショットの数が指定数を超えると、最も古いスナップショットが最初に削除されます。  最大保持値は 1018 です。保持期間がONTAPバージョンでサポートされている値よりも高い値に設定されている場合、バックアップは失敗します。  SnapshotコピーベースのバックアップでSnapVaultレプリケーションを有効にする場合は、保持数を2以上に設定する必要があります。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。  SAP HANAシステム レプリケーションでは、SAP HANAシステムのすべてのリソースを1つのリソース グループに追加することを推奨します。これにより、適切な数のバックアップが保持されます。  SAP HANAシステム レプリケーションでは、作成されるSnapshotの総数はリソース グループに設定された保持数と同じになります。最も古いSnapshotが削除されるかどうかは、最も古いSnapshotが配置されているノードに基づいて決まります。たとえば、SAP HANAシステム レプリケーション プライマリとSAP HANAシステム レプリケーション セカンダリが含まれているリソース グループの保持数が7に設定されているとします。一度に作成できるSnapshotの数は、SAP HANAシステム レプリケーション プライマリとSAP HANAシステム レプリケーション セカンダリの両方を合わせて最大で7つです。

状況	操作
Snapshotを特定の日数だけ保持	*コピーの保持期間*を選択し、スナップショットを削除する前に保持する日数を指定します。
スナップショットコピーのロック期間	スナップショット コピーのロック期間 を選択し、日、月、または年を指定します。 SnapLock保持期間は100年未満にする必要があります。

8. Snapshotラベルを選択します。



リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしなくても実行できます。

9. スナップショット コピー ベースのバックアップの場合、[セカンダリ レプリケーション オプションの選択] セクションで、次のセカンダリ レプリケーション オプションの 1 つまたは両方を選択します。

フィールド	操作
ローカル スナップショット コピーを作成した後、 SnapMirror を更新します	別のボリュームにバックアップ セットのミラー コピーを作成する場合（SnapMirrorレプリケーション）は、このフィールドを選択します。 このオプションは、SnapMirrorアクティブ同期に対して有効にする必要があります。 ONTAPの保護関係のタイプがミラーとバックアップの場合、このオプションのみを選択すると、プライマリで作成されたSnapshotがデスティネーションに転送されませんが、デスティネーションのリストに表示されます。このSnapshotがリストア処理の対象としてデスティネーションで選択されると、「Secondary Location is not available for the selected vaulted/mirrored backup」というエラー メッセージが表示されます。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。 トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 見る"TopologyページでのSAP HANAデータベースのバックアップとクローンの表示"]。

フィールド	操作
ローカルスナップショットコピーを作成した後、 SnapVault を更新します	ディスクツーディスクのバックアップ レプリケーション (SnapVaultバックアップ) を実行する場合は、このオプションを選択します。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 SnapLock がSnapLock Vault と呼ばれるONTAPのセカンダリにのみ設定されている場合、[トポロジ] ページの [更新] ボタンをクリックすると、ONTAPから取得されたセカンダリのロック期間が更新されます。 SnapLock Vaultの詳細については、"バックアップ デスティネーションのSnapshotコピーのWORM状態へのコミット" 見る"[Topology] ページでのSAP HANAデータベースのバックアップとクローンの表示"。
エラー再試行回数	処理が停止されるまでに試行できるレプリケーションの最大回数を入力します。



セカンダリ ストレージでSnapshotの上限に達しないように、ONTAPでセカンダリ ストレージのSnapMirror保持ポリシーを設定する必要があります。

10. 概要を確認し、[完了] をクリックします。

リソース グループの作成とポリシーの適用

リソース グループはコンテナであり、バックアップして保護するリソースをここに追加する必要があります。リソース グループを使用することで、特定のアプリケーションに関連するすべてのデータを同時にバックアップできます。リソース グループはいずれのデータ保護ジョブにも必要になります。リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義することも必要です。

タスク概要

- SAP HANAシステム レプリケーションのバックアップを作成するには、SAP HANAシステムのすべてのリソースを1つのリソース グループに追加することを推奨します。これにより、テイクオーバー / フェイルバック モードでのシームレスなバックアップが保証されます。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

- SnapMirrorアクティブ同期を使用するリソースを含む既存のリソース グループにSnapMirrorアクティブ同期を使用しない新しいデータベースを追加することはできません。
- SnapMirrorアクティブ同期のフェイルオーバー モードである既存のリソース グループに新しいデータベースを追加することはできません。リソースを追加できるのは、通常の状態またはフェイルバック状態のリソース グループのみです。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。

フィールド	操作
Name	リソース グループの名前を入力します。  リソース グループ名は250文字以内で指定する必要があります。
Tags	リソース グループを検索しやすくするために、ラベルを入力します。 たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。
Use custom name format for Snapshot copy	Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。 たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付け加えられます。

4. [リソース] ページで、[ホスト] ドロップダウン リストからホスト名を選択し、[リソース タイプ] ドロップダウン リストからリソース タイプを選択します。

画面の情報がフィルタリングされます。

5. *利用可能なリソース*セクションからリソースを選択し、右矢印をクリックして*選択したリソース*セクションに移動します。
6. [Application Settings] ページで、次の操作を実行します。
 - a. 追加のバックアップ オプションを設定するには、[バックアップ] 矢印をクリックします。

整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for Consistency Group Snapshot operation to complete	スナップショット操作が完了するまでの待機時間を指定するには、「緊急」、「中」、または「緩和」を選択します。 [Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

+

- *スクリプト*矢印をクリックし、静止、スナップショット、および静止解除操作の事前コマンドと事後コマンドを入力します。障害の発生時に終了前に実行するプリコマンドも入力できます。
- *カスタム構成*矢印をクリックし、このリソースを使用するすべてのデータ保護操作に必要なカスタムのキーと値のペアを入力します。

パラメータ	設定	説明
ARCHIVE_LOG_ENABLE	(Y / N)	アーカイブ ログ管理を有効にし、アーカイブ ログを削除します。

パラメータ	設定	説明
ARCHIVE_LOG_RETENTION	number_of_days	アーカイブ ログを保持する日数を指定します。 この設定は、NTAP_SNAPSHOT_RETENTIONS 以上である必要があります。
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブ ログが含まれるディレクトリへのパスを指定します。
ARCHIVE_LOG_EXT	file_extension	アーカイブ ログ ファイルの拡張子の長さを指定します。 たとえば、アーカイブ ログが log_backup_0_0_0_0.161518551942 9 で、file_extension 値が 5 の場合、ログの拡張子は 5 桁、つまり 16151 になります。
ARCHIVE_LOG_RECURSIVE_SEARCH	(Y / N)	サブディレクトリ内のアーカイブ ログの管理を有効にします。 アーカイブ ログがサブディレクトリの下にある場合は、このパラメータを使用する必要があります。



カスタムのキーと値のペアは、SAP HANA Linuxプラグイン システムではサポートされますが、一元化されたWindowsプラグインとして登録されたSAP HANAデータベースではサポートされません。

- c. スナップショット コピー ツールの矢印をクリックして、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する（このオプションはLinuxリソースには適用されません）	ファイル システムの一貫性を備えたSnapCenter * を選択します。 このオプションは、SnapCenter Plug-in for SAP HANA Databaseには適用されません。
SnapCenterでストレージ レベルのSnapshotを作成する	ファイル システムの整合性のないSnapCenter * を選択します。

あなたが望むなら...	操作
Snapshotコピーを作成するためにホストで実行するコマンドを入力する	*その他*を選択し、スナップショットを作成するためにホスト上で実行するコマンドを入力します。

7. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます 。

ポリシーが[Configure schedules for selected policies]セクションのリストに表示されます。

- b. スケジュールの設定列で*をクリックします。  * 設定するポリシーの。
- c. ポリシー *policy_name* のスケジュールの追加ダイアログ ボックスでスケジュールを構成し、[OK] をクリックします。

*policy_name*は、選択したポリシーの名前です。

構成されたスケジュールは、「適用されたスケジュール」列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP サーバーは、設定 > グローバル設定 で設定する必要があります。

9. 概要を確認し、[完了] をクリックします。

リソース グループを作成し、**ASA r2** システム上の **SAP HANA** リソースの二次保護を有効にする

ASA r2 システム上にあるリソースを追加するには、リソース グループを作成する必要があります。リソース グループの作成時にセカンダリ保護をプロビジョニングすることもできます。

開始する前に

- ONTAP 9.x リソースとASA r2 リソースの両方を同じリソース グループに追加していないことを確認する必要があります。
- ONTAP 9.x リソースとASA r2 リソースの両方を含むデータベースが存在しないことを確認する必要があります。

タスク概要

- 二次保護は、ログインしたユーザーに **SecondaryProtection** 機能が有効になっているロールが割り当てられている場合にのみ使用できます。
- セカンダリ保護を有効にすると、プライマリおよびセカンダリ整合性グループの作成中にリソース グループはメンテナンス モードになります。プライマリおよびセカンダリのコンシステンシー グループが作成されると、リソース グループのメンテナンス モードが解除されます。
- SnapCenter はクローン リソースの二次保護をサポートしていません。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。

- a. [Name] フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag] フィールドに1つ以上のラベルを入力します。

たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

- c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- d. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。



必要に応じて、プレフィックスを含め、アプリケーションで設定されたのと同じ宛先を使用する必要があります。

4. [リソース] ページで、[ホスト] ドロップダウン リストからデータベース ホスト名を選択します。



[Available Resources] セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources] のリストには表示されません。

5. [使用可能なリソース] セクションからASA r2 リソースを選択し、[選択したリソース] セクションに移動します。
6. アプリケーション設定ページで、バックアップ オプションを選択します。
7. [Policies] ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックし  でポリシーを作成することもできます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。
- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 選択したポリシーに対して二次保護が有効になっている場合は、「二次保護」ページが表示されるので、次の手順を実行する必要があります。
 - a. レプリケーション ポリシーのタイプを選択します。



同期レプリケーション ポリシーはサポートされていません。

- b. 使用する整合性グループのサフィックスを指定します。
- c. [宛先クラスタ] および [宛先 SVM] ドロップダウンから、使用するピア クラスタと SVM を選択します。



クラスタと SVM のピアリングはSnapCenterではサポートされていません。クラスタと SVM のピアリングを実行するには、System Manager またはONTAP CLI を使用する必要があります。



リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは [セカンダリ保護リソース] セクションに表示されます。

1. [Verification]ページで、次の手順を実行します。
 - a. ロケーターのロード をクリックして、 SnapMirrorまたはSnapVaultボリュームをロードし、セカンダリストレージで検証を実行します。
 - b. クリック  ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で をクリックします。
 - c. [Add Verification Schedules *policy_name*]ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

- d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証] を選択します。
- e. [OK]をクリックします。

設定した検証スケジュールが、[Applied Schedules]列にリストされます。

2. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtptServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

3. 概要を確認し、[完了] をクリックします。

SAP HANAデータベース用のPowerShellコマンドレットを使用したストレージ システムへの接続とクレデンシャルの作成

PowerShellコマンドレットを使用してSAP HANAデータベースのバックアップ、リストア、クローニングを行う前に、Storage Virtual Machine (SVM) 接続とクレデンシャルを作成する必要があります。

開始する前に

- PowerShellコマンドレットを実行できるようにPowerShell環境を準備しておく必要があります。
- ストレージ接続を作成するには、Infrastructure Adminロールの権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

ストレージ システム接続の追加中は、ホスト プラグインのインストールが進行中であってはなりません。ホスト キャッシュが更新されず、SnapCenter GUI にデータベースのステータスが「バックアップに使用できません」または「NetAppストレージ上にありません」と表示される可能性があるためです。

- ストレージ システムの名前は一意である必要があります。

SnapCenterでは、別々のクラスタに属している場合でも、複数のストレージ システムに同じ名前を付けることはサポートされません。SnapCenterでサポートする各ストレージ システムには、一意な名前とデータLIFの一意なIPアドレスが必要です。

手順

1. Open-SmConnectionコマンドレットを使用して、PowerShell接続セッションを開始します。

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

2. Add-SmStorageConnectionコマンドレットを使用して、ストレージ システムへの新しい接続を作成します。


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

3. Add-SmCredentialコマンドレットを使用して、新しいクレデンシャルを作成します。

この例は、Windowsクレデンシャルを使用してFinanceAdminという名前の新しいクレデンシャルを作成する方法を示しています。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. SnapCenter ServerにSAP HANA通信ホストを追加します。

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName  
FinanceAdmin -PluginCode hana
```

5. パッケージとSnapCenter Plug-in for SAP HANA Databaseをホストにインストールします。

Linux :

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode  
hana
```

Windows :

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana  
-FileSystemCode scw -RunAsName FinanceAdmin
```

6. HDBSQLクライアントのパスを設定します。

Windows :

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode  
hana -configSettings @"HANA_HDBSQL_CMD" = "C:\Program  
Files\sap\hdbclient\hdbsql.exe"
```

Linux :

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com  
-PluginCode hana -configSettings  
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

SAP HANAデータベースのバックアップ

どのリソース グループにもまだ含まれていないリソースは、[Resources]ページからバックアップすることができます。

開始する前に

- バックアップ ポリシーを作成しておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。
- Snapshotコピーベースのバックアップ処理の場合は、すべてのテナント データベースが有効でアクティブであることを確認してください。
- SAP HANAシステム レプリケーションのバックアップを作成するには、SAP HANAシステムのすべてのリソースを1つのリソース グループに追加することを推奨します。これにより、テイクオーバー / フェイルバック モードでのシームレスなバックアップが保証されます。

"[リソース グループの作成とポリシーの適用](#)"。

"[リソース グループのバックアップ](#)"

- 1つ以上のテナントデータベースがダウンしているときにファイルベースのバックアップを作成する場合は、HANAプロパティファイルでALLOW_FILE_BASED_BACKUP_IFINACTIVE_TENANTS_PRESENTパラメータを*YES*に設定します。`Set-SmConfigSettings`コマンドレット。

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行することで取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"

- 休止、Snapshot、および休止解除の処理を実行するプリコマンドとポストコマンドの場合は、プラグインホストで次のパスから使用できるコマンド リストにコマンドがあるかどうかを確認する必要があります。
 - Windows ホスト上のデフォルトの場所: *C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Linux ホスト上のデフォルトの場所: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*



コマンドがコマンド リストに存在しない場合、処理は失敗します。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. リソース ページで、リソース タイプに基づいて 表示 ドロップダウン リストからリソースをフィルターします。

を選択 、ホスト名とリソース タイプを選択して、リソースをフィルターします。次に選択できます  フィルター パネルを閉じます。

3. バックアップするリソースを選択します。
4. [リソース] ページで、[スナップショット コピーにカスタム名形式を使用する] を選択し、スナップショット名に使用するカスタム名形式を入力します。

たとえば、`customtext_policy_hostname` または `resource_hostname` です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

5. [Application Settings] ページで、次の操作を実行します。

- 追加のバックアップ オプションを設定するには、[バックアップ] 矢印を選択します。

必要に応じて、整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for "Consistency Group Snapshot" operation to complete	スナップショット操作が完了するまでの待機時間を指定するには、「緊急」、または「中」、または「緩和」を選択します。[Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

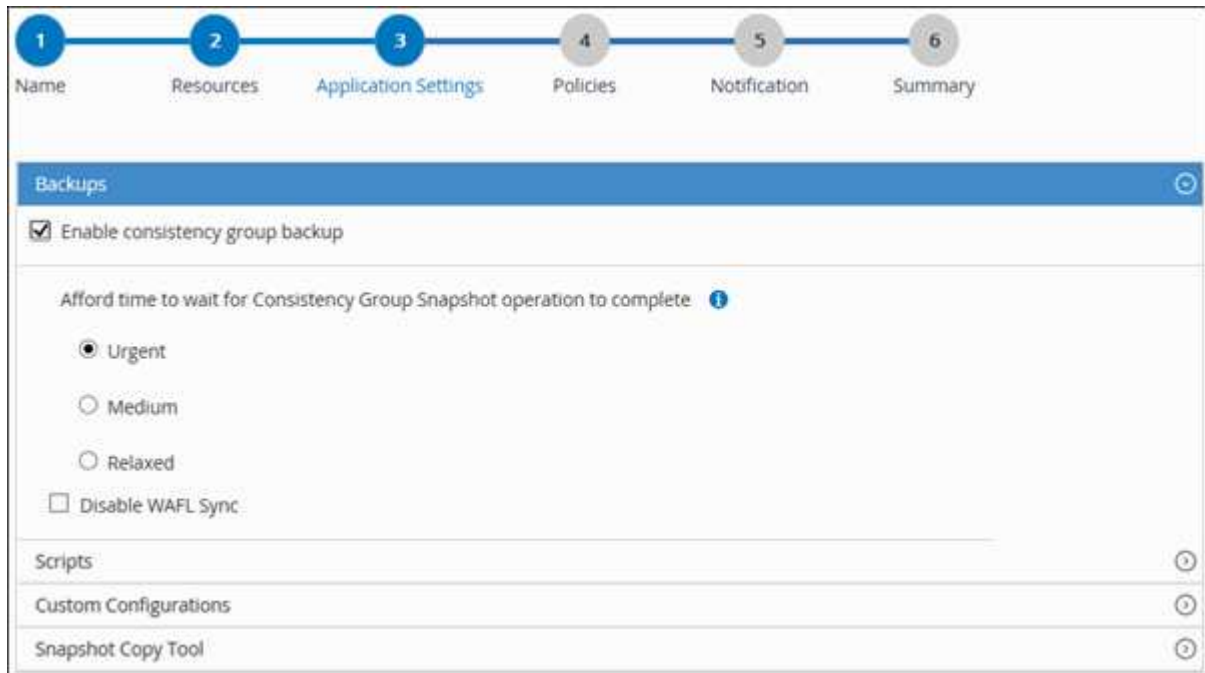
- *スクリプト*矢印を選択して、静止、スナップショット、および静止解除操作の事前および事後コマンドを実行します。

バックアップ処理を終了する前のプリコマンドも実行できます。プリスクリプトとポストスクリプトはSnapCenter Serverで実行されます。

- カスタム構成矢印を選択し、このリソースを使用するすべてのジョブに必要なカスタム値のペアを入力します。
- スナップショット コピー ツール 矢印を選択して、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでストレージ レベルのSnapshotを作成する	• ファイル システムの整合性のないSnapCenter * を選択します。

あなたが望むなら...	操作
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する	ファイル システムの一貫性を備えたSnapCenter * を選択します。
Snapshotを作成するためのコマンドを入力する	*その他*を選択し、スナップショットを作成するコマンドを入力します。



6. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます 。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b.  を選択
スケジュールを構成するポリシーの [スケジュールの構成] 列で、
- c. ポリシー *policy_name* のスケジュールの追加 ダイアログ ボックスでスケジュールを構成し、[OK] を選択します。

policy_name は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

7. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。

す。SMTP は、設定 > グローバル設定 でも設定する必要があります。

8. 概要を確認し、[完了] を選択します。

リソースのトポロジ ページが表示されます。

9. *今すぐバックアップ*を選択します。

10. [Backup]ページで次の手順を実行します。

- a. リソースに複数のポリシーを適用した場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*を選択します。

11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

- MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

詳細については、以下を参照してください。 ["MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"](#)

- VMDK上のアプリケーション データをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープ サイズが不足していると、バックアップが失敗することがあります。

Java ヒープ サイズを増やすには、スクリプト ファイル `/opt/netapp/init_scripts/scvservice` を見つけます。このスクリプトでは、`do_start method` コマンドによってSnapCenter VMware プラグイン サービスが開始されます。このコマンドを次のように更新します: `Java -jar -Xmx8192M -Xms4096M`

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-smconnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\
```

ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmResourcesコマンドレットを使用して、リソースを追加します。

この例は、SingleContainerタイプのSAP HANAデータベースを追加する方法を示しています。

```
C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
-DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
(@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary"
}) -SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys
'HS10' -osdbuser 'h10adm' -filebackupprefix 'H10_'
```

この例は、MultipleContainersタイプのSAP HANAデータベースを追加する方法を示しています。

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType
MultipleContainers -StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.net
app.com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType
'MultiTenant'
```

次の例は、データ ボリューム以外のリソースを作成する方法を示しています。

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sscore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Add-SmPolicyコマンドレットを使用して、バックアップ ポリシーを作成します。

この例では、Snapshotコピーベースのバックアップのバックアップ ポリシーを作成しています。

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType
Backup -PluginPolicyType hana -BackupType SnapShotBasedBackup
```

この例では、ファイルベースのバックアップのバックアップ ポリシーを作成しています。

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
-PluginPolicyType hana -BackupType FileBasedBackup
```

4. リソースを保護するか、Add-SmResourceGroupコマンドレットを使用してSnapCenterに新しいリソース グループを追加します。

この例では、単一コンテナのリソースを保護しています。

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

この例では、複数コンテナのリソースを保護しています。

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies
hana_snapshotbased,hana_Filebased
-Resources @{"Host"="host.example.com";"UID"="MDC\SID"}
-Description test -usesnapcenterwithoutfilesystemconsistency
```

この例では、ポリシーとリソースを指定して新しいリソース グループを作成しています。

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sscore.test.com";"Uid"="SID"},@{"Host"="sc
corelinux62.sscore.test.com";"Uid"="MDC\SID"})
-Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency -plugincode 'HANA'
```

この例では、データ ボリューム以外のリソース グループを作成します。

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="H11";"PluginName"=
"hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="MDC\H31";"Pl
uginName"="hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="No
nDataVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

5. New-SmBackupコマンドレットを使用して、新しいバックアップ ジョブを開始します。

この例は、リソース グループをバックアップする方法を示しています。

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

この例では、保護されたリソースをバックアップしています。

```
C:\PS> New-SMBackup -Resources  
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}  
-Policy hana_Filebased
```

6. Get-smJobSummaryReport コマンドレットを使用して、ジョブのステータス（実行中、完了、失敗）を確認します。

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Get-SmBackupReport コマンドレットを使用して、リストアやクローニングの処理を実行するバックアップIDとバックアップ名など、バックアップ ジョブの詳細を監視します。

```
PS C:\> Get-SmBackupReport -JobId 351  
Output:  
BackedUpObjects           : {DB1}  
FailedObjects             : {}  
IsScheduled               : False  
HasMetadata               : False  
SmBackupId                : 269  
SmJobId                   : 2361  
StartDateTime             : 10/4/2016 11:20:45 PM  
EndDateTime               : 10/4/2016 11:21:32 PM  
Duration                  : 00:00:46.2536470  
CreatedDateTime           : 10/4/2016 11:21:09 PM  
Status                    : Completed  
ProtectionGroupName       : Verify_ASUP_Message_windows  
SmProtectionGroupId       : 211  
PolicyName                : test2  
SmPolicyId                : 20  
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-  
2016_23.20.46.2758  
VerificationStatus        : NotVerified  
VerificationStatuses      :  
SmJobError                :  
BackupType                : SCC_BACKUP  
CatalogingStatus          : NotApplicable  
CatalogingStatuses        :  
ReportDataCreatedDateTime :
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

リソース グループのバックアップ

リソース グループは、ホスト上のリソースの集まりです。リソース グループのバックアップ処理は、リソース グループに定義されているすべてのリソースを対象に実行されます。

開始する前に

- ポリシーを適用したリソース グループを作成しておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。

タスク概要

リソース グループは、[Resources]ページからオンデマンドでバックアップできます。リソース グループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが行われます。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。

リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、をクリックして、タグを選択します。次に選択できます  フィルター パネルを閉じます。

3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] を選択します。
4. [Backup] ページで次の手順を実行します。

- a. リソース グループに複数のポリシーを関連付けた場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*を選択します。

5. モニター > ジョブ を選択して、操作の進行状況を監視します。

SAP HANAデータベースのバックアップ処理の監視

SnapCenterの[Jobs]ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

-  進行中

-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*ジョブ*をクリックします。
3. [Jobs]ページで、次の手順を実行します。
 - a. をクリックして、 リストの内容をバックアップ処理だけに絞り込みます。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*バックアップ*を選択します。
 - d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. バックアップ ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスは  ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[Activity]ペインでのSAP HANAデータベースに対するデータ保護処理の監視

[Activity]ペインには、最後に実行された5つの処理が表示されます。また[Activity]ペインには、処理が開始された日次と処理のステータスが表示されます。

[Activity]ペインには、バックアップ、リストア、クローニング、スケジュールされたバックアップの各処理に関する情報が表示されます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. クリック  アクティビティ ペインで、最新の 5 つの操作を表示します。

いずれかの操作をクリックすると、*ジョブの詳細*ページに操作の詳細が表示されます。

SAP HANAのバックアップ処理のキャンセル

キューに登録されているバックアップ処理はキャンセルできます。

必要なもの

- 処理をキャンセルするには、SnapCenter管理者がジョブ所有者としてログインする必要があります。
- バックアップ操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のバックアップ処理はキャンセルできません。
- バックアップ処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。
- キャンセルできない操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたバックアップ操作をキャンセルできます。

手順

1. 次のいずれかを実行します。

方法	アクション
[Monitor]ページ	a. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 b. 操作を選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	a. バックアップ操作を開始したら、*をクリックします。 * アクティビティ ペインで、最新の 5 つの操作を表示します。 b. 処理を選択します。 c. ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

処理がキャンセルされ、リソースは処理前の状態に戻ります。

[Topology]ページでのSAP HANAデータベースのバックアップとクローンの表示

リソースのバックアップまたはクローニングを準備する際に、プライマリ ストレージとセカンダリ ストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。

タスク概要

プライマリ ストレージまたはセカンダリ ストレージ（ミラー コピーまたはバックアップ コピー）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

•



プライマリ ストレージで使用可能なバックアップとクローンの数を表示します。

-  SnapMirrorテクノロジーを使用してセカンダリ ストレージにミラーリングされているバックアップとクローンの数を表示します。
-  SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップとクローンの数を表示します。



表示されるバックアップの数には、セカンダリ ストレージから削除されたバックアップも含まれます。たとえば、バックアップを4個保持するポリシーを使用してバックアップを6個作成した場合、バックアップの数は6個と表示されます。



mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジ ビューに表示されますが、トポロジ ビューのミラー バックアップの数にはバージョンに依存しないバックアップは含まれません。

[Topology]ページでは、選択したリソースまたはリソース グループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を参照し、対象を選択してデータ保護処理を実行できます。

SnapMirrorアクティブ同期 (当初はSnapMirror Business Continuity [SM-BC] としてリリース) としてセカンダリ関係がある場合は、次の追加アイコンが表示されます。

-  レプリカサイトが稼働しています。
-  レプリカサイトはダウンしています。
-  セカンダリ ミラーまたはボルト関係が再確立されていません。

手順

- 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
- [リソース] ページで、[表示] ドロップダウン リストからリソースまたはリソース グループを選択します。
- リソースの詳細ビューまたはリソース グループの詳細ビューで、リソースを選択します。

リソースが保護されている場合は、選択したリソースのトポロジ ページが表示されます。

- *概要カード*を確認して、プライマリ ストレージとセカンダリ ストレージで使用可能なバックアップとクローンの数の概要を確認します。

概要カード セクションには、ファイルベースのバックアップ、スナップショット コピー ベースのバックアップ、およびクローンの合計数が表示されます。

更新 ボタンをクリックすると、ストレージのクエリが開始され、正確な数が表示されます。

SnapLock対応バックアップが取得された場合、[更新] ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでも、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

アプリケーション リソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限はONTAPから取得されます。

SnapMirrorアクティブ同期の場合、[更新] ボタンをクリックすると、プライマリ サイトとレプリカ サイトの両方に対してONTAP を照会してSnapCenterバックアップ インベントリが更新されます。週次スケジュールでも、SnapMirrorアクティブ同期関係を含むすべてのデータベースに対してこの処理が実行されます。

- SnapMirrorアクティブ同期とONTAP（バージョン9.14.1のみ）では、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップの関係については、フェイルオーバー後に手動で設定する必要があります。ONTAP 9.15.1以降は、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップが、自動的に設定されます。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。バックアップが作成された後にのみ、「更新」をクリックできます。

5. 「コピーの管理」ビューで、プライマリ ストレージまたはセカンダリ ストレージから バックアップ または クローン をクリックして、バックアップまたはクローンの詳細を表示します。

バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、削除の各処理を実行します。



セカンダリ ストレージ上のバックアップは、名前変更または削除できません。

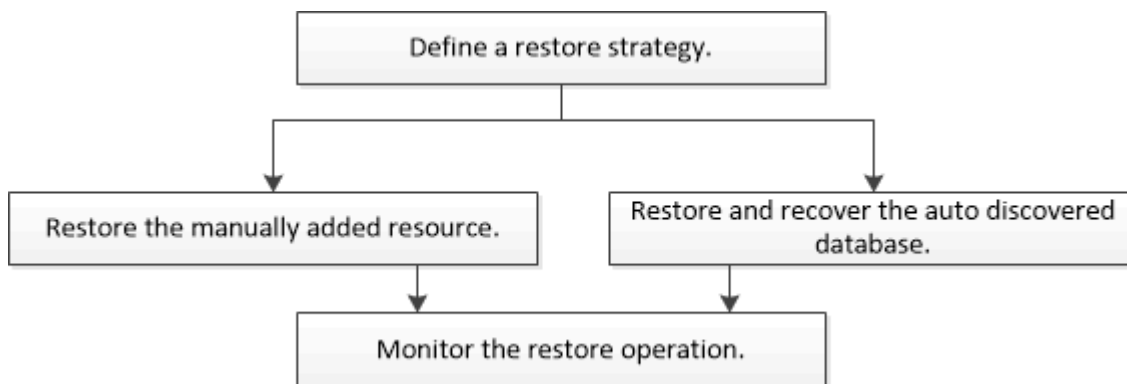
7. クローンを削除する場合は、表でクローンを選択し、 をクリックします。
8. クローンを分割する場合は、テーブルからクローンを選択し、。

SAP HANAデータベースのリストア

リストアのワークフロー

リストアとリカバリのワークフローには、計画、リストア処理の実行、および処理の監視が含まれます。

次のワークフローは、リストア処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処

理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

手動で追加されたリソース バックアップのリストアとリカバリ

SnapCenterを使用して1つまたは複数のバックアップからデータをリストアおよびリカバリすることができます。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- リストアするリソースまたはリソース グループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- リストア前、リストア後、マウント、アンマウントの各コマンドを実行する場合は、プラグイン ホストで次のパスから使用可能なコマンド リストにコマンドが存在するかどうかを確認する必要があります。
 - Windows ホスト上のデフォルトの場所: `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux ホスト上のデフォルトの場所: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- ファイルベースのバックアップのコピーをSnapCenterからリストアすることはできません。
- SnapCenter 4.3へのアップグレード後は、SnapCenter 4.2で作成したバックアップのリストアはできますが、リカバリはできません。SnapCenter 4.2で作成したバックアップをリカバリするには、HANA StudioまたはSnapCenter外部のHANAリカバリ スクリプトを使用する必要があります。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期でリストア処理を実行するには、プライマリの場所からバックアップを選択する必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホスト、関連するリソース グループとポリシー、およびステータスとともに表示されます。



リストアの実行時は、バックアップがリストア グループに対するものであっても、リストア対象のリソースを個別に選択する必要があります。

リソースが保護されていない場合は、「全体ステータス」列に「保護されていません」と表示されます。この状態になるのは、リソースが保護されていない場合とリソースが別のユーザによってバックアップされている場合です。

3. リソースを選択するか、リソース グループを選択してそのグループ内のリソースを選択します。

リソースのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージ システムから [バックアップ] を選択します。
5. プライマリバックアップテーブルで、復元するバックアップを選択し、*をクリックします。  *。

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scspr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. [復元範囲] ページで、[完全なリソース] または [ファイル レベル] のいずれかを選択します。

- a. *完全なリソース*を選択すると、SAP HANA データベースのすべての構成済みデータ ボリュームが復元されます。

リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeのリストア用のSnapshotが選択されたあとに作成されたSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。

- b. *ファイルレベル*を選択した場合は、*すべて*を選択するか、特定のボリュームまたはqtreeを選択して、それらのボリュームまたはqtreeに関連するパスをカンマで区切って入力することができます。

- ボリュームとqtreeは複数選択できます。
- リソース タイプがLUNの場合は、LUN全体がリストアされます。

複数のLUNを選択できます。



すべてを選択すると、ボリューム、qtree、または LUN 上のすべてのファイルが復元されます。

7. [Pre ops]ページで、リストア ジョブの実行前に実行するリストア前の処理とアンマウントのコマンドを入力します。

自動検出されたリソースにはアンマウント コマンドを使用できません。

8. [Post ops]ページで、リストア ジョブの実行後に実行するマウントとリストア後の処理のコマンドを入力します。

自動検出されたリソースにはマウント コマンドを使用できません。

9. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP は、[設定] > [グローバル設定] ページでも設定する必要があります。

10. 概要を確認し、[完了] をクリックします。

11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよびGet-SmBackupReportコマンドレットを使用して、リストアする1つまたは複数のバックアップに関する情報を取得します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackupコマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

自動検出されたデータベース バックアップのリストアとリカバリ

SnapCenterを使用して1つまたは複数のバックアップからデータをリストアおよびリカバリすることができます。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- リストアするリソースまたはリソース グループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- リストア前、リストア後、マウント、アンマウントの各コマンドを実行する場合は、プラグイン ホストで次のパスから使用可能なコマンド リストにコマンドが存在するかどうかを確認する必要があります。

- Windows ホスト上のデフォルトの場所: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux ホスト上のデフォルトの場所: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- ファイルベースのバックアップのコピーをSnapCenterからリストアすることはできません。
- SnapCenter 4.3へのアップグレード後は、SnapCenter 4.2で作成したバックアップのリストアはできますが、リカバリはできません。SnapCenter 4.2で作成したバックアップをリカバリするには、HANA Studio またはSnapCenter外部のHANAリカバリ スクリプトを使用する必要があります。
- ONTAP 9.12.1 以前のバージョンでは、復元の一環としてSnapLock Vault スナップショットから作成されたクローンには、SnapLock Vault の有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期でリストア処理を実行するには、プライマリの場所からバックアップを選択する必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホスト、関連するリソース グループとポリシー、およびステータスとともに表示されます。



リストアの実行時は、バックアップがリストア グループに対するものであっても、リストア対象のリソースを個別に選択する必要があります。

リソースが保護されていない場合は、「全体ステータス」列に「保護されていません」と表示されます。この状態になるのは、リソースが保護されていない場合とリソースが別のユーザによってバックアップされている場合です。

3. リソースを選択するか、リソース グループを選択してそのグループ内のリソースを選択します。

リソースのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボールド化された) ストレージシステムから [バックアップ] を選択します。

5. プライマリバックアップテーブルで、復元するバックアップを選択し、*をクリックします。  *

Primary Backup(s)	
search 	  
Backup Name	End Date
rg1_scspr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. 「復元範囲」ページで、「完全なリソース」を選択して、SAP HANA データベースの構成済みデータ ボリュームを復元します。



完全なリソース (ボリュームの復元*の有無にかかわらず)、または *テナント データベース のいずれかを選択できます。

ユーザーが テナント データベース または 完全復元 オプションのいずれかを選択した場合、 SnapCenter Server では複数のテナントに対するリカバリ操作はサポートされません。リカバリ処理を実行するには、HANA StudioまたはHANA Pythonスクリプトを使用する必要があります。

- a. ボリューム全体を復元する場合は、「ボリュームを元に戻す」を選択します。

このオプションは、NFS環境のSnapCenter 4.3で作成されたバックアップで使用できます。

リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeのリストア用のSnapshotが選択されたあとに作成されたSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。これは、復元に ボリュームの復元 オプション付きの 完全なリソース が選択されている場合に適用されます。

- b. テナント データベース を選択します。

このオプションは、MDCリソースに対してのみ使用できます。

リストア処理を実行する前に、テナント データベースを停止してください。

テナント データベース オプションを選択した場合は、HANA スタジオを使用するか、 SnapCenter外部の HANA リカバリ スクリプトを使用してリカバリ操作を実行する必要があります。

7. [Recovery scope]ページで、次のいずれかのオプションを選択します。

状況	操作
現在の時刻にできる限り近い時点にリカバリする場合	*最新の状態に回復*を選択します。単一コンテナ リソースの場合は、ログおよびカタログ バックアップの場所を1つ以上指定します。 マルチテナント データベース コンテナ (MDC) リソースの場合は、ログ バックアップの場所を1つ以上とバックアップ カタログの場所を指定します。 MDCリソースの場合、パスにシステム データベースとテナント データベースの両方のログが含まれている必要があります。

状況	操作
指定した時点にリカバリする場合	*特定の時点に回復*を選択します。 a. タイムゾーンを選択します。 ブラウザのタイムゾーンがデフォルトで入力されます。 入力した時間は、選択したタイムゾーンに基づいてGMTに変換されます。 b. 日時を入力します。たとえば、HANA Linuxホストがカリフォルニア州サニーベールにあり、ノースカロライナ州ローリーにいるユーザーがログをSnapCenterにリカバリしようとしているとします。 これらの地点間の時差は3時間で、ユーザーはノースカロライナ州ローリーからログインしているため、GUIで選択されるデフォルトのブラウザ タイムゾーンはGMT-04:00です。 ユーザーがカリフォルニア州サニーベールの午前5時にリカバリを実行したい場合、ユーザーはブラウザのタイムゾーンをHANA Linuxホストのタイムゾーン（GMT-07:00）に設定し、日付と時刻を午前5時に指定する必要があります。 単一コンテナ リソースの場合は、ログおよびカタログ バックアップの場所を1つ以上指定します。 MDCリソースの場合は、ログ バックアップの場所を1つ以上とバックアップ カタログの場所を指定します。 MDCリソースの場合、パスにシステム データベースとテナント データベースの両方のログが含まれている必要があります。
特定の日時までリカバリする場合	*指定されたデータ バックアップに復元*を選択します。
リカバリが不要である場合	*回復なし*を選択します。リカバリ処理は、HANA Studioから手動で実行する必要があります。

SnapCenter 4.3へのアップグレード後に作成されたバックアップのみをリカバリできます。ただし、ホストとプラグインの両方がSnapCenter 4.3にアップグレードされており、リストア対象として選択されたバックアップの作成がリソースの変換またはリソースの自動検出後に行われた場合に限りです。

8. [Pre ops]ページで、リストア ジョブの実行前に実行するリストア前の処理とアンマウントのコマンドを入力します。

自動検出されたリソースにはアンマウント コマンドを使用できません。

9. [Post ops]ページで、リストア ジョブの実行後に実行するマウントとリストア後の処理のコマンドを入力します。

自動検出されたリソースにはマウント コマンドを使用できません。

10. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP は、[設定]>[グローバル設定] ページでも設定する必要があります。

11. 概要を確認し、[完了] をクリックします。

12. モニター>ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレットを使用したリソースのリストア

リソースのバックアップをリストアするときは、SnapCenter Serverとの接続セッションを開始し、バックアップをリストしてバックアップの情報を取得し、バックアップをリストアします。

PowerShellコマンドレットを実行できるように環境を準備しておく必要があります。

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよびGet-SmBackupReportコマンドレットを使用して、リストアする1つまたは複数のバックアップに関する情報を取得します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----

1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDateTime "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackup コマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

SAP HANAデータベースのリストア処理の監視

[Job]ページを使用して、SnapCenterの各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中

-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  てリストをフィルタリングし、リストア処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*復元*を選択します。
 - d. *ステータス*ドロップダウンリストから、復元ステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. 復元ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

SAP HANAリソースのバックアップのクローニング

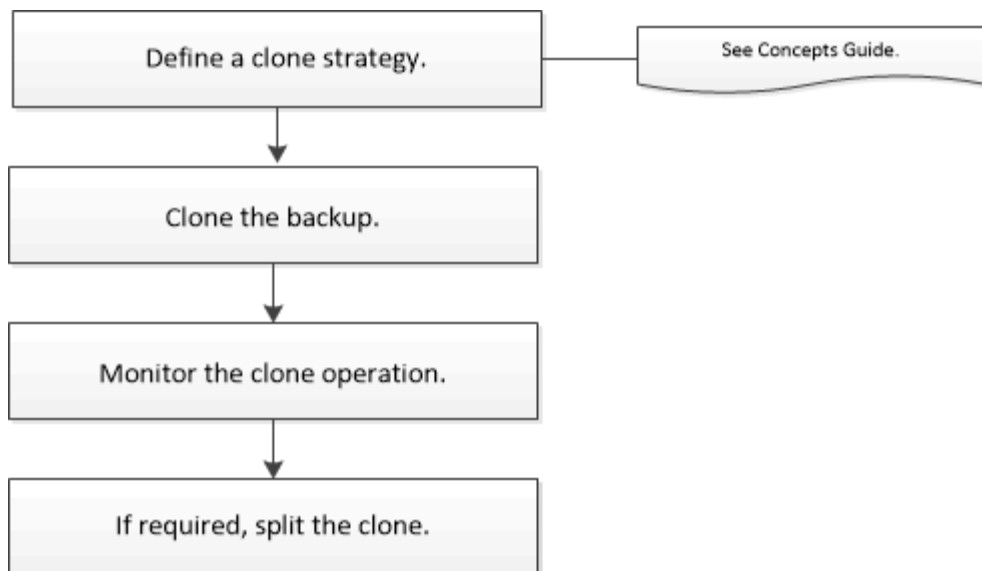
クローニングのワークフロー

クローニング ワークフローには、クローニング処理の実行と処理の監視が含まれます。

タスク概要

- ソースSAP HANAサーバでクローニング処理を実行できます。
- リソースのバックアップをクローニングする理由には次のものがあります。
 - アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のリソースの構造およびコンテンツを使用してテストするため
 - データの抽出と操作を行うツールで、データ ウェアハウスにデータを取り込むため
 - 誤って削除または変更されたデータをリカバリするため

次のワークフローは、クローニング処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

SAP HANAデータベースのバックアップのクローニング

SnapCenterを使用してバックアップをクローニングすることができます。クローニングはプライマリとセカンダリのどちらのバックアップからも実行できます。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- ボリュームをホストするアグリゲートがStorage Virtual Machine (SVM) の割り当て済みアグリゲート リストに含まれていることを確認します。
- ファイルベースのバックアップはクローニングできません。
- ターゲットのクローン サーバのSAP HANAインスタンスSIDは、[Target Clone SID]フィールドで指定したSIDと同じである必要があります。
- クローニング前またはクローニング後のコマンドについては、プラグイン ホストの次のパスで使用できるコマンド リストにコマンドが存在するかどうかを確認する必要があります。
 - Windows の場合: `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linuxの場合: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- クローン分割操作の制限については、以下を参照してください。"[ONTAP 9 論理ストレージ管理ガイド](#)"。
- ONTAP 9.12.1 以前のバージョンでは、復元の一環としてSnapLock Vault スナップショットから作成されたクローンには、 SnapLock Vault の有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホスト、関連するリソース グループとポリシー、ステータスなどの情報とともに表示されます。

3. リソースまたはリソース グループを選択します。

リソース グループを選択した場合はリソースを選択する必要があります。

リソースまたはリソース グループのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージ システムから [バックアップ] を選択します。
5. 表からデータバックアップを選択し、クリックします。 。
6. [Location] ページで、次の操作を実行します。

フィールド	操作
プラグインホスト	クローンのマウント先のプラグインがインストールされたホストを選択します。
Target Clone SID	既存のバックアップからクローニングするSAP HANAインスタンスIDを入力します。
NFS Export IP Address	クローン ボリュームをエクスポートするホスト名またはIPアドレスを入力します。
iSCSI Initiator	LUNのエクスポート先ホストのiSCSIイニシエータ名を入力します。このオプションは、LUNリソース タイプを選択した場合にのみ使用できます。
プロトコル	LUNプロトコルを入力します。このオプションは、LUNリソース タイプを選択した場合にのみ使用できます。

リソースとしてLUNを選択し、セカンダリ バックアップからクローニングする場合、デスティネーション ボリュームのリストが表示されます。1つのソースについて複数のデスティネーション ボリュームを選択することができます。



クローニングを実行する前に、iSCSIイニシエータまたはFCPが存在し、設定が完了し、代替ホストにログインしていることを確認します。

7. [Scripts]ページで、次の手順を実行します。



スクリプトはプラグイン ホストで実行されます。

- a. クローニング処理の前後に実行するプリコマンドやポストコマンドを入力します。
 - クローニング前のコマンド：同じ名前の既存のデータベースの削除
 - クローニング後のコマンド：データベースの検証やデータベースの起動
- b. ホストにファイルシステムをマウントするには、mountコマンドを入力します。

Linuxマシンのボリュームまたはqtreeに対するmountコマンド：

NFSの例: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。

9. 概要を確認し、[完了] をクリックします。

10. モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-SmConnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

2. Get-SmBackupコマンドレットを使用して、クローニング処理を実行するバックアップを取得します。

この例では、クローニングできるバックアップが2つあります。

```
C:\PS> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
1	Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM	

3. 既存のバックアップからクローニング処理を開始し、クローニングされたボリュームをエクスポートするNFSエクスポートのIPアドレスを指定します。

この例では、NFSExportIPsのアドレスを10.232.206.169と指定してバックアップをクローニングしています。

```
New-SmClone -AppPluginCode hana -BackupName
scsccore1_sccore_test_com_hana_H73_scsccore1_06-07-
2017_02.54.29.3817 -Resources
@{"Host"="scsccore1.sccore.test.com";"Uid"="H73"} -CloneToInstance
shivsc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data'
-preclonecreatecommands '/home/scripts/scpre_clone.sh'
-postclonecreatecommands '/home/scripts/scpost_clone.sh'
```



NFSExportIPsを指定しない場合、デフォルトでクローン ターゲット ホストにエクスポートされます。

4. Get-SmCloneReportコマンドレットを使用してクローニング ジョブの詳細を表示し、バックアップが正常にクローニングされたことを確認します。

クローンID、開始日時、終了日時などの詳細を確認できます。

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration             : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName           : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName     : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources      : {Don, Betty, Bobby, Sally}
ClonedResources       : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError           :
```

SAP HANAデータベースのクローニング処理の監視

SnapCenterのクローニング処理の進捗状況を、[Jobs]ページで監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  てリストをフィルタリングし、クローニング処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*クローン*を選択します。
 - d. *ステータス*ドロップダウンリストからクローンのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. クローンジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. ジョブの詳細ページで、*ログの表示*をクリックします。

クローンのスプリット

SnapCenterを使用して、クローン リソースを親リソースからスプリットできます。スプリットされたクローンは親リソースから独立します。

タスク概要

- 中間クローンではクローン スプリット処理を実行できません。

たとえば、データベース バックアップからクローン1を作成したあとで、クローン1のバックアップを作成し、そのバックアップ（クローン2）をクローニングできます。クローン2を作成すると、クローン1は中間クローンになり、クローン1ではクローン スプリット処理を実行できなくなります。ただし、クローン2に対してはクローン スプリット処理を実行できます。

クローン2をスプリットすると、クローン1は中間クローンではなくなるため、クローン1に対してクローン スプリット処理を実行できるようになります。

- クローンをスプリットすると、そのクローンのバックアップ コピーとクローン ジョブが削除されます。
- FlexCloneボリューム分割操作の詳細については、以下を参照してください。 ["親ボリュームからのFlexCloneボリュームのスプリット"](#)。
- ストレージ システム上のボリュームまたはアグリゲートがオンラインであることを確認します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. *リソース*ページで、表示リストから適切なオプションを選択します。

オプション	説明
データベース アプリケーションの場合	表示リストから*データベース*を選択します。
ファイルシステムの場合	表示リストから*パス*を選択します。

3. リストから適切なリソースを選択します。

リソースのトポロジ ページが表示されます。

4. *コピーの管理*ビューから、クローンされたリソース（データベースやLUNなど）を選択し、*をクリックします。  *。
5. 分割するクローンの推定サイズとアグリゲート上で必要な空き容量を確認し、[開始] をクリックします。
6. モニター > ジョブ をクリックして、操作の進行状況を監視します。

SMCoreサービスが再起動されると、クローン スプリット処理は応答を停止します。Stop-SmJobコマンドレットを実行してクローン スプリット処理を停止してから、クローン スプリット処理を再試行してください。

クローンが分割されているかどうかを確認するためのポーリング時間を長くしたり短くしたりする場合は、SMCoreServiceHost.exe.config ファイルの CloneSplitStatusCheckPollTime パラメータの値を変更して、SMCore がクローン分割操作のステータスをポーリングする時間間隔を設定できます。値はミリ秒単位で、デフォルト値は5分です。

例えば：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

バックアップ、リストア、または別のクローン スプリットが実行中の場合、クローン スプリットの開始処理は失敗します。クローン スプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

["アグリゲートが存在しないためにSnapCenterのクローニングや検証が失敗する"](#)

SnapCenterアップグレード後のSAP HANAデータベースのクローンの削除またはスプリット

SnapCenter 4.3にアップグレードすると、クローンは表示されなくなります。クローンを作成したリソースの[Topology]ページで、クローンの削除やスプリットを実行できます。

タスク概要

非表示のクローンのストレージ フットプリントを見つける場合は、次のコマンドを実行します。 `Get-SmClone -ListStorageFootprint`

手順

1. `remove-smbbackup` コマンドレットを使用して、クローニングされたリソースのバックアップを削除します。
2. `remove-smresourcegroup` コマンドレットを使用して、クローニングされたリソースのリソース グループを削除します。
3. `remove-smprotectresource` コマンドレットを使用して、クローニングされたリソースの保護を解除します。
4. [Resources] ページで親リソースを選択します。

リソースのトポロジ ページが表示されます。

5. [Manage Copies] ビューで、プライマリまたはセカンダリ（ミラー先またはレプリケート先）ストレージ システムからクローンを選択します。
6. クローンを選択し、クリックします  クローンを削除するには、または  クローンを分割します。
7. [OK] をクリックします。

Oracleデータベースの保護

SnapCenter Plug-in for Oracle Databaseの概要

Plug-in for Oracle Databaseの機能

SnapCenter Plug-in for Oracle Databaseは、Oracleデータベースに対してアプリケーション対応のデータ保護管理を可能にする、NetApp SnapCenterソフトウェアのホスト側コンポーネントです。

Plug-in for Oracle Databaseによって、SnapCenter環境でのOracleデータベースのバックアップ、Oracle Recovery Manager (RMAN) を使用したカタログ化とカタログ化解除、検証、マウント、アンマウント、リストア、リカバリ、クローニングを自動化できます。Plug-in for Oracle Databaseは、すべてのデータ保護処理を実行するためにSnapCenter Plug-in for UNIXをインストールします。

Plug-in for Oracle Databaseでは、SAPアプリケーションを実行しているOracleデータベースのバックアップを管理することもできます。ただし、SAP BR*Toolsとの統合はサポートされません。

- データファイル、制御ファイル、およびアーカイブ ログ ファイルをバックアップします。

バックアップは、コンテナ データベース (CDB) レベルでのみサポートされます。

- データベース、コンテナ データベース (CDB) 、プラガブル データベース (PDB) のリストアとリカバリを行います。

PDBの不完全リカバリはサポートされていません。

- ある時点までの本番環境データベースのクローンを作成します。

クローニングはCDBレベルでのみサポートされます。

- バックアップをすぐに検証します。
- リカバリ処理のためにデータ バックアップとログ バックアップのマウントとアンマウントを行います。
- バックアップ処理と検証処理をスケジュールします。
- すべての処理を監視します。
- バックアップ、リストア、クローニングの各処理のレポートを表示します。
- SnapCenter環境のOracleデータベースに対するアプリケーション対応のバックアップ、リストア、リカバリ、検証、マウント、アンマウント、クローニングの各処理が自動化されます。
- SAP用のOracleデータベースをサポートしますが、SAP BR*Toolsとの統合は提供されません。

Plug-in for Oracle Databaseの機能

Plug-in for Oracle Databaseは、LinuxまたはAIXホスト上でOracleデータベースと統合されるほか、ストレージ システム上でNetAppのテクノロジーと統合されます。

- 統一されたグラフィカル ユーザ インターフェイス

SnapCenterのインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。どのプラグインでも、SnapCenterのインターフェイスから、バックアップ、リストア、リカバリ、クローニングの各処理を一貫した方法で実行できるほか、ダッシュボード ビューで概要を把握したり、ロールベース アクセス制御（RBAC）を設定したり、ジョブを監視したりすることができます。

- 自動化された全体管理

バックアップ処理とクローン処理のスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理を実行したりできます。SnapCenterからのEメール アラートの送信を設定して、環境をプロアクティブに監視することもできます。

- 無停止のNetApp Snapshotテクノロジー

SnapCenterでは、Plug-in for Oracle DatabaseおよびPlug-in for UNIXでNetApp Snapshotテクノロジーを使用してデータベースがバックアップされます。Snapshotはストレージ スペースを最小限しか消費しません。

Plug-in for Oracle Databaseには、次の利点もあります。

- バックアップ、リストア、クローニング、マウント、アンマウント、検証の各処理のワークフローがサポートされます。
- ホスト上に構成されたOracleデータベースの自動検出
- Oracle Recovery Manager（RMAN）を使用したカタログ化とカタログ化解除がサポートされます。
- セキュリティがRBACでサポートされ、ロール委譲が一元化されます。

クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルのアクセス権を付与することもできます。

- リストア処理とクローニング処理でのアーカイブ ログ管理（ALM）のサポート
- NetApp FlexCloneテクノロジーを使用して、テストまたはデータ抽出に使用する本番環境データベースのコピー（スペース効率に優れたポイントインタイム コピー）を作成できます。

クローンを作成するストレージ システムにFlexCloneライセンスが必要です。

- SAN環境およびASM環境でバックアップを作成する際に、ONTAPの整合グループ（CG）機能がサポートされます。
- 自動化された無停止のバックアップ検証を利用できます。
- 複数のデータベース ホストで同時に複数のバックアップを実行できます。

1回の処理で、1つのホストの複数のデータベースが同じボリュームを共有する場合に複数のSnapshotが統合されます。

- 物理インフラと仮想インフラがサポートされます。
- NFS、iSCSI、ファイバチャネル（FC）、RDM、NFSおよびVMFS経由のVMDK、NFS、SAN、RDM、およびVMDK経由のASMがサポートされます。
- ONTAPの選択的LUNマップ（SLM）機能がサポートされます。

デフォルトで有効になるSLM機能は、最適パスを持たないLUNを定期的に検出して修正します。SLMを設定するには、`/var/opt/snapcenter/scu/etc`にある`scu.properties`ファイルのパラメータを変更します。

- `ENABLE_LUNPATH_MONITORING` パラメータの値を `false` に設定することで、これを無効にすることができます。
- `LUNPATH_MONITORING_INTERVAL` パラメータに値 (時間単位) を割り当てることで、LUN パスが自動的に修正される頻度を指定できます。SLMの詳細については、"[ONTAP 9 SAN管理セクション](#)"。

- LinuxでNon-Volatile Memory express (NVMe) がサポートされます。

- NVMeユーティリティがホストにインストールされている必要があります。

代替ホストにクローニングまたはマウントするには、NVMeユーティリティをインストールする必要があります。

- バックアップ、リストア、クローニング、マウント、アンマウント、カタログ化、カタログ化解除、検証の処理は、RDMなどの仮想環境を除き、NVMeハードウェアでサポートされます。

上記の処理は、パーティションのないデバイスまたは単一パーティションのデバイスでサポートされています。



NVMeデバイス用にマルチパス ソリューションを設定するには、カーネルでネイティブ マルチパス オプションを設定します。デバイス マッパー (DM) マルチパスはサポートされていません。

- NVMe over TCP/IPでは、バックアップ、リストア、クローニング、マウント、アンマウント、カタログ化、カタログ化解除、検証の各ワークフローがサポートされます。
- NVMe over TCP/IP上に作成されたVMDKレイアウトでは、バックアップ、リストア、クローニング、マウント、アンマウント、カタログ化、カタログ化解除、検証の各ワークフローがサポートされます。

- サイト全体の障害時でもビジネス サービスの運用を継続できるようにするSnapMirrorアクティブ シンク (当初はSnapMirror Business Continuity [SM-BC] としてリリース) をサポートし、セカンダリ コピーを使用してアプリケーションを透過的にフェイルオーバーできるようにします。SnapMirrorアクティブ同期でフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。
- デフォルト (oracleとgrid) 以外の任意のユーザをサポートします。

デフォルト以外のユーザーをサポートするには、`file /var/opt/snapcenter/sco/etc/`にある **sco.properties** ファイル内のパラメーターの値を変更して、デフォルト以外のユーザーを設定する必要があります。

パラメータのデフォルト値はoracleおよびgridに設定されています。

- `DB_USER=oracle`
- `DB_GROUP=oinstall`
- `GI_USER=grid`
- `GI_GROUP=oinstall`

Plug-in for Oracle Databaseでサポートされるストレージ タイプ

SnapCenterは、物理マシンと仮想マシンの両方でさまざまなストレージ タイプをサポートしています。SnapCenter Plug-ins Package for LinuxまたはSnapCenter Plug-ins Package for AIXをインストールする前に、ストレージ タイプがサポートされていること

を確認する必要があります。

SnapCenterでは、LinuxおよびAIXのストレージ プロビジョニングはサポートされていません。

Linuxでサポートされるストレージ タイプ

次の表に、Linuxでサポートされるストレージ タイプを示します。

マシン	ストレージ タイプ
物理サーバ	• FC接続LUN • iSCSI接続LUN • NFS接続ボリューム • NVMe-FC • NVMe/TCP
VMware ESXi	• FCまたはiSCSI HBAで接続されたRDM LUNホスト バス アダプタ (HBA) のスキャン は、SnapCenterがホストに存在するすべてのホスト バス アダプタをスキャンするため、完了までに時間がかかることがあります。 <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> にある LinuxConfig.pm ファイルを編集し て、SCSI_HOSTS_OPTIMIZED_RESCAN パラメータの値を 1 に設定し、HBA_DRIVER_NAMES にリストされているHBA のみを再スキャンすることができます。 • iSCSIイニシエータでゲスト システムに直接接続されたiSCSI LUN • NFSデータストア上のVMDK • NVMe/TCP 経由で作成された VMFS 上の VMDK  RACは、共有VMDKをサポートするESX 8.0U2でサポートされません。 • ゲスト システムに直接接続されたNFSボリューム • NFSとSANの両方に存在するvVolデータストア vVolデータストアは、ONTAP Tools for VMware vSphereでのみプロビジョニングできます。

AIXでサポートされるストレージ タイプ

次の表に、AIXでサポートされるストレージ タイプを示します。

マシン	ストレージ タイプ
物理サーバ	• FC接続およびiSCSI接続のLUN SAN環境では、ASM、LVM、SANファイルシステムがサポートされます。  AIXおよびファイルシステムでのNFSはサポートされていません。 • 拡張ジャーナリング ファイルシステム (JFS2) SANファイルシステムおよびLVMレイアウトでのインライン ロギングをサポートします。

その "[NetApp Interoperability Matrix Tool](#)"サポートされているバージョンに関する最新情報が含まれています。

Plug-in for OracleでのSnapMirrorレプリケーションとSnapVaultレプリケーションのためのストレージ システムの準備

SnapCenterプラグインと一緒にONTAP SnapMirrorテクノロジーを使用すると、バックアップセットのミラー コピーを別のボリュームに作成できます。また、ONTAP SnapVaultを使用すれば、標準への準拠やその他のガバナンスを目的としたディスクツーディスクのバックアップ レプリケーションを実行できます。これらのタスクを実行する前に、ソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenterは、Snapshot処理の完了後に、SnapMirrorとSnapVaultに対する更新を実行します。SnapMirror更新とSnapVault更新は、SnapCenterジョブの一部として実行されるため、ONTAPスケジュールを別途作成しないでください。



NetApp SnapManager製品からSnapCenterに移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリ ストレージ（ソース ボリューム）上のデータがセカンダリ ストレージ（デスティネーション ボリューム）にレプリケートされます。この関係を初期化すると、ソース ボリュームで参照されるデータ ブロックがデスティネーション ボリュームに転送されます。



SnapCenter は、SnapMirrorとSnapVaultボリューム間のカスケード関係をサポートしていません（* プライマリ * > ミラー > ボールト）。ファンアウト関係を使用する必要があります。

SnapCenterは、バージョンに依存しないSnapMirror関係の管理をサポートしています。バージョンに依存しないSnapMirror関係とその設定方法の詳細については、"[ONTAPのドキュメント](#)"。

Plug-in for Oracleに必要な最小限のONTAP権限

必要な最小ONTAP権限は、データ保護に使用するSnapCenterプラグインによって異なります。

- 全アクセス コマンド: ONTAP 9.12.1 以降に必要な最小限の権限

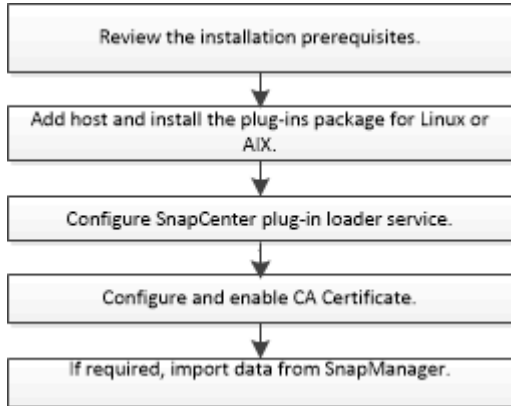
- event generate-autosupport-log
- job history show
- job stop
- lun
- lun attribute show
- lun create
- lun delete
- lun geometry
- lun igroup add
- lun igroup create
- lun igroup delete
- lun igroup rename
- lun igroup show
- lun mapping add-reporting-nodes
- lun mapping create
- lun mapping delete
- lun mapping remove-reporting-nodes
- lun mapping show
- lun modify
- lun move-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- lun resize
- lun serial
- lun show
- snapmirror policy add-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- snapmirror restore
- snapmirror show

- snapmirror show-history
- snapmirror update
- snapmirror update-ls-set
- snapmirror list-destinations
- version
- volume clone create
- volume clone show
- volume clone split start
- volume clone split stop
- volume create
- volume destroy
- volume file clone create
- volume file show-disk-usage
- volume offline
- volume online
- volume modify
- volume qtree create
- volume qtree delete
- volume qtree modify
- volume qtree show
- volume restrict
- volume show
- volume snapshot create
- volume snapshot delete
- volume snapshot modify
- volume snapshot rename
- volume snapshot restore
- volume snapshot restore-file
- volume snapshot show
- volume unmount
- SVM
- vserver cifs
- vserver cifs shadowcopy show
- vserver show
- ネットワークインターフェース
- network interface show
- metrocluster show

SnapCenter Plug-in for Oracle Databaseのインストール

SnapCenter Plug-in for Oracle Databaseのインストール ワークフロー

Oracle データベースを保護する場合は、Oracle データベース用のSnapCenterプラグインをインストールして設定する必要があります。



ホストを追加して**Plug-in Package for Linux / AIX**をインストールするための前提条件

ホストを追加してプラグイン パッケージをインストールする前に、すべての要件を満たしておく必要があります。

- iSCSIを使用している場合は、iSCSIサービスが実行されている必要があります。
- rootユーザまたはroot以外のユーザに対してパスワード ベースのSSH接続を有効にしておく必要があります。

SnapCenter Plug-in for Oracle Databaseは、root以外のユーザもインストールできます。ただし、プラグイン プロセスをインストールして開始できるよう、root以外のユーザにsudo権限を設定する必要があります。プラグインのインストール後、プロセスは有効なroot以外のユーザとして実行されます。

- AIXホストにSnapCenter Plug-ins Package for AIXをインストールする場合は、ディレクトリ レベルのシンボリック リンクを手動で解決しておく必要があります。

ファイル レベルのシンボリック リンクはSnapCenter Plug-ins Package for AIXで自動的に解決されますが、JAVA_HOMEの絶対パスを取得するためのディレクトリ レベルのシンボリック リンクは解決されません。

- インストール ユーザのクレデンシャルを、認証モードをLinuxまたはAIXに設定して作成します。
- Java 11をLinuxホストまたはAIXホストにインストールしておく必要があります。
 - OracleのJavaとOpenJDKはLinuxでサポートされています
 - AIX 用の IBM Java。ダウンロードはこちらから ["IBM Semeru ランタイムのダウンロード"](#)



LinuxホストにJava 11の認定エディションのみがインストールされていることを確認します。

- LinuxまたはAIXホストでOracleデータベースを実行している場合は、SnapCenter Plug-in for Oracle

DatabaseとSnapCenter Plug-in for UNIXの両方をインストールする必要があります。



Plug-in for Oracle Databaseは、SAP用のOracleデータベースの管理にも使用できます。ただし、SAP BR*Toolsとの統合はサポートされません。

- Oracleデータベース11.2.0.3以降を使用している場合は、13366202 Oracleパッチをインストールする必要があります。



/etc/fstabファイルのUUIDマッピングは、SnapCenterではサポートされていません。

- プラグインのインストールには、デフォルトのシェルとして **bash** を使用する必要があります。

Linuxホストの要件

SnapCenter Plug-ins Package for Linuxをインストールする前に、ホストが要件を満たしていることを確認する必要があります。

項目	要件
オペレーティング システム	• Red Hat Enterprise Linux • Oracle Linux  Oracle LinuxまたはRed Hat Enterprise Linux 6.6 / 7.0オペレーティング システムのLVMでOracleデータベースを使用している場合は、最新バージョンの論理ボリューム マネージャ (LVM) をインストールする必要があります。 • SUSE Linux Enterprise Server (SLES)
ホスト上のSnapCenterプラグインに必要な最小RAM	2 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	2 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。

項目	要件
必要なソフトウェア パッケージ	Java 11 Oracle と OpenJDK  LinuxホストにJava 11の認定エディションのみがインストールされていることを確認します。 Javaを最新バージョンにアップグレードした場合は、/var/opt/snapcenter/spl/etc/spl.propertiesにあるJAVA_HOMEオプションが正しいJavaバージョンと正しいパスに設定されていることを確認する必要があります。

サポートされているバージョンに関する最新情報については、["NetApp Interoperability Matrix Tool"](#)。

Linuxホストのroot以外のユーザへのsudo権限の設定

SnapCenter 2.0以降のリリースでは、root以外のユーザがSnapCenter Plug-ins Package for Linuxをインストールしてプラグイン プロセスを開始できます。プラグイン プロセスは有効なroot以外のユーザとして実行されます。いくつかのパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

必要なもの

- sudoバージョン1.8.7以降
- umask が 0027 の場合、java フォルダーとその中のすべてのファイルに 555 の権限があることを確認します。そうしないと、プラグインのインストールが失敗する可能性があります。
- root以外のユーザについては、root以外のユーザの名前とユーザのグループが同じであることを確認してください。
- /etc/ssh/sshd_config ファイルを編集して、メッセージ認証コード アルゴリズム (MAC hmac-sha2-256 および MAC hmac-sha2-512) を設定します。

この構成ファイルを更新したら、sshdサービスを再起動します。

例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

このタスクについて

次のパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /custom_location/NetApp/snapcenter/spl/bin/spl

手順

1. SnapCenter Plug-ins Package for LinuxをインストールするLinuxホストにログインします。
2. visudo Linuxユーティリティを使用して、/etc/sudoersファイルに次の行を追加します。

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,  
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,  
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc  
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/Linux_Prechecks.sh  
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config  
_Check.sh  
Cmnd_Alias SCCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/bin/sc_command_executor  
Cmnd_Alias SCCMDEXECUTOR =checksum_value==  
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor  
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,  
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD  
Defaults: LINUX_USER env_keep += "IATEMPDIR"  
Defaults: LINUX_USER env_keep += "JAVA_HOME"  
Defaults: LINUX_USER !visiblepw  
Defaults: LINUX_USER !requiretty
```



RAC をセットアップしている場合は、他の許可されたコマンドとともに、/etc/sudoers ファイルに次の行を追加する必要があります: '<crs_home>/bin/olsnodes'

crs_home の値は、/etc/oracle/olr.loc ファイルから取得できます。

LINUX_USER は、作成した非 root ユーザーの名前です。

checksum_value は、次の場所にある **sc_unix_plugins_checksum.txt** ファイルから取得できます。

- SnapCenter Server が Windows ホストにインストールされている場合は、C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt。
- SnapCenter Server が Linux ホストにインストールされている場合は、/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt。



この例は、独自のデータを作成する際の参照としてのみ使用してください。

AIXホストの要件

SnapCenter Plug-ins Package for AIXをインストールする前に、ホストが要件を満たしていることを確認する必要があります。



SnapCenter Plug-ins Package for AIXに含まれているSnapCenter Plug-in for UNIXでは、同時ボリューム グループはサポートされません。

項目	要件
オペレーティング システム	AIX 7.1以降
ホスト上のSnapCenterプラグインに必要な最小RAM	4 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	2 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	Java 11 IBM Java Javaを最新バージョンにアップグレードした場合は、/var/opt/snapcenter/spl/etc/spl.propertiesにあるJAVA_HOMEオプションが正しいJavaバージョンと正しいパスに設定されていることを確認する必要があります。

サポートされているバージョンに関する最新情報については、["NetApp Interoperability Matrix Tool"](#)。

AIXホストのroot以外のユーザへのsudo権限の設定

SnapCenter 4.4以降では、root以外のユーザがSnapCenter Plug-ins Package for AIXをインストールしてプラグイン プロセスを開始できます。プラグイン プロセスは有効なroot以外のユーザとして実行されます。いくつかのパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

必要なもの

- sudoバージョン1.8.7以降
- umask が 0027 の場合、java フォルダーとその中のすべてのファイルに 555 の権限があることを確認します。そうしないと、プラグインのインストールが失敗する可能性があります。

- `/etc/ssh/sshd_config` ファイルを編集して、メッセージ認証コード アルゴリズム (MAC hmac-sha2-256 および MAC hmac-sha2-512) を設定します。

この構成ファイルを更新したら、sshdサービスを再起動します。

例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

このタスクについて

次のパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

- `/home/AIX_USER/sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/custom_location/NetApp/snapcenter/spl/bin/spl`

手順

1. SnapCenter Plug-ins Package for AIXをインストールするAIXホストにログインします。
2. visudo Linuxユーティリティを使用して、`/etc/sudoers`ファイルに次の行を追加します。

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



RAC をセットアップしている場合は、他の許可されたコマンドとともに、`/etc/sudoers` ファイルに次の行を追加する必要があります: `'/<crs_home>/bin/olsnodes'`

`crs_home` の値は、`/etc/oracle/olr.loc` ファイルから取得できます。

`AIX_USER` は、作成した非 root ユーザーの名前です。

`checksum_value` は、次の場所にある `sc_unix_plugins_checksum.txt` ファイルから取得できます。

- SnapCenter Server が Windows ホストにインストールされている場合は、`C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`。
- SnapCenter Server が Linux ホストにインストールされている場合は、`/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`。



この例は、独自のデータを作成する際の参照としてのみ使用してください。

クレデンシャルの設定

SnapCenterは、クレデンシャルを使用してSnapCenterの処理を実行するユーザを認証します。LinuxまたはAIXホストにプラグイン パッケージをインストールするためのクレデンシャルを作成する必要があります。

このタスクについて

rootユーザ、またはプラグイン プロセスをインストールして開始するsudo権限があるroot以外のユーザに対してクレデンシャルを作成します。

詳細については、以下を参照してください。 [Linuxホストのroot以外のユーザへのsudo権限の設定](#) または [AIXホストのroot以外のユーザへのsudo権限の設定](#)

ベスト プラクティス: ホストをデプロイしてプラグインをインストールした後でも認証情報を作成できますが、ベスト プラクティスとしては、SVM を追加した後、ホストをデプロイしてプラグインをインストールする前に認証情報を作成します。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定] ページで、[資格情報] をクリックします。
3. *新規* をクリックします。
4. [Credential] ページで、クレデンシャル情報を入力します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。
ユーザー名/パスワード	認証に使用するユーザ名とパスワードを入力します。 • ドメイン管理者 SnapCenterプラグインをインストールするシステムのドメイン管理者を指定します。[Username] フィールドの有効な形式は次のとおりです。 ◦ <i>NetBIOS</i>\ユーザー名 ◦ ドメイン<i>FQDN</i>\ユーザー名 • ローカル管理者（ワークグループの場合のみ） ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。ユーザー名フィールドの有効な形式は次のとおりです: <i>UserName</i>
Authentication Mode	使用する認証モードを選択します。 プラグイン ホストのオペレーティング システムに応じて、LinuxまたはAIXのどちらかを選択します。
Use sudo privileges	非 root ユーザーの資格情報を作成する場合は、[sudo 権限を使用する] チェックボックスをオンにします。

5. [OK]をクリックします。

資格情報の設定が完了したら、[ユーザーとアクセス] ページでユーザーまたはユーザー グループに資格情報のメンテナンスを割り当てることができます。

Oracleデータベースのクレデンシャルの設定

Oracleデータベースに対してデータ保護処理を実行する際に使用するクレデンシャルを設定する必要があります。

このタスクについて

Oracleデータベースでサポートされているさまざまな認証方式を確認してください。詳細については、"[クレデンシャルの認証方式](#)"。

個々のリソース グループのクレデンシャルを設定する際、ユーザ名に完全なadmin権限が割り当てられていない場合は、少なくともリソース グループとバックアップの権限をそのユーザ名に割り当てる必要があります。

Oracleデータベース認証が有効になっている場合は、リソース ビューに赤いロック アイコンが表示されます。データベースを保護できるようにデータベースのクレデンシャルを設定するか、またはデータベースをリソース グループに追加してデータ保護処理を実行する必要があります。



クレデンシャルの作成時に間違った詳細を指定すると、エラー メッセージが表示されます。* キャンセル*をクリックして再試行する必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] を選択します。
3. をクリックし 、ホスト名とデータベース タイプを選択してリソースをフィルタします。

そのあとに  をクリックすると、フィルタ ペインが閉じます。

4. データベースを選択し、[データベース設定] > [データベースの構成] をクリックします。
5. データベース設定の構成セクションで、*既存の資格情報の使用* ドロップダウン リストから、Oracle データベースでデータ保護ジョブを実行するために使用する資格情報を選択します。



Oracleユーザにはsysdba権限が必要です。

クリックして認証情報を作成することもできます 。

6. ASM 設定の構成セクションで、既存の資格情報の使用 ドロップダウン リストから、ASM インスタンスでデータ保護ジョブを実行するために使用する資格情報を選択します。



ASMユーザにはsysasm権限が必要です。

クリックして認証情報を作成することもできます 。

7. RMAN カタログ設定の構成セクションで、既存の資格情報の使用 ドロップダウン リストから、Oracle

Recovery Manager (RMAN) カタログ データベースでデータ保護ジョブを実行するために使用する資格情報を選択します。

クリックして認証情報を作成することもできます 。

TNSName フィールドに、SnapCenterサーバーがデータベースと通信するために使用する Transparent Network Substrate (TNS) ファイル名を入力します。

- 優先 **RAC** ノード フィールドで、バックアップに優先する Real Application Cluster (RAC) ノードを指定します。

RACデータベース インスタンスが存在するいずれかまたはすべてのクラスター ノードを指定できます。バックアップ処理は、指定したノードでのみ、指定した順序で実行されます。

RAC One Nodeでは、優先ノードに表示されるノードは1つだけで、この優先ノードはデータベースが現在ホストされているノードです。

RAC One Node データベースのフェイルオーバーまたは再配置後、SnapCenter のリソース ページでリソースを更新すると、データベースが以前にホストされていた 優先 **RAC** ノード リストからホストが削除されます。データベースが再配置される RAC ノードは **RAC** ノード にリストされ、優先 RAC ノードとして手動で構成する必要があります。

詳細については、以下を参照してください。 ["RACセットアップにおける優先ノード"](#)。

- [OK]をクリックします。

GUIを使用してホストを追加し、**Plug-ins Package for Linux / AIX**をインストールする

[Add Host]ページを使用してホストを追加し、SnapCenter Plug-ins Package for LinuxまたはSnapCenter Plug-ins Package for AIXをインストールできます。プラグインは、自動的にリモート ホストにインストールされます。

このタスクについて

ホストの追加とプラグイン パッケージのインストールは、ホストごとまたはクラスターごとに実行できます。クラスター (Oracle RAC) にプラグインをインストールする場合、プラグインはクラスターのすべてのノードにインストールされます。Oracle RAC One Nodeの場合は、このプラグインをアクティブ ノードとパッシブ ノードの両方にインストールする必要があります。



Oracle RACにプラグインをインストールする際は、パスワードベースの認証のみがサポートされます。SSHキーベースの認証はサポートされていません。

この処理を実行するためには、SnapCenter Adminロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられている必要があります。



SnapCenter Serverをプラグイン ホストとして別のSnapCenter Serverに追加することはできません。

手順

- 左側のナビゲーション ペインで、[ホスト] をクリックします。

2. 上部の*管理対象ホスト*タブが選択されていることを確認します。
3. *[追加]*をクリックします。
4. [Hosts]ページで、次の操作を実行します。

フィールド	操作
ホストタイプ	ホスト タイプとして Linux または AIX を選択します。 SnapCenter Serverがホストを追加し、Plug-in for Oracle DatabaseとPlug-in for UNIXをホストにインストールします（プラグインがまだインストールされていない場合）。
ホスト名	ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。 SnapCenterが機能するためには、DNSが適切に設定されている必要があります。そのため、FQDNを入力することを推奨します。 次のいずれかのIPアドレスまたはFQDNを入力できます。 • スタンドアロン ホスト • Oracle Real Application Clusters（RAC）環境内の任意のノード  ノードVIPやSCAN IPはサポートされていません。 SnapCenterを使用してサブドメインの一部であるホストを追加する場合は、FQDNを指定する必要があります。
Credentials	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモート ホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。  クレデンシャルの認証モードは、[Add Host]ウィザードで指定するホスト タイプによって決まります。

5. [Select Plug-ins to Install]セクションで、インストールするプラグインを選択します。

6. (オプション) [その他のオプション] をクリックします。

フィールド	操作
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。 デフォルトのポート番号は8145です。SnapCenter Serverがカスタム ポートにインストールされている場合は、そのポート番号がデフォルト ポートとして表示されます。  プラグインを手動でインストールしてカスタム ポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理が失敗します。
Installation Path	デフォルトのパスは <code>/opt/ NetApp/snapcenter</code> です。 必要に応じて変更できます。
Oracle RAC内のすべてのホストを追加します	Oracle RAC内のすべてのクラスタ ノードを追加するには、このチェック ボックスをオンにします。 Flex ASMセットアップでは、ハブ ノードかリーフ ノードかに関係なく、すべてのノードが追加されます。
Skip optional preinstall checks	プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェック ボックスをオンにします。

7. *送信*をクリックします。

[Skip prechecks]チェック ボックスをオンにしていない場合、プラグインをインストールするための要件を満たしているかどうかを確認するために、ホストが検証されます。



事前確認スクリプトでは、ファイアウォールの拒否ルールに指定されているプラグイン ポートのファイアウォール ステータスは検証されません。

最小要件を満たしていない場合、エラーまたは警告メッセージが表示されます。エラーがディスク容量または RAM に関連している場合は、`C:\Program Files\ NetApp\ SnapCenter WebApp` にある `web.config` ファイルを更新してデフォルト値を変更できます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。



HAのセットアップでweb.configファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. 指紋を確認して、「確認して送信」をクリックします。

クラスター セットアップでは、クラスター内の各ノードのフィンガープリントを検証する必要があります。



SnapCenterでは、ECDSAアルゴリズムがサポートされていません。



前述の手順で同じホストがSnapCenterに追加され、フィンガープリントが確認された場合でも、フィンガープリントの検証は必須です。

9. インストールの進捗状況を監視します。

インストール固有のログ ファイルは、`/custom_location/snapcenter/logs` にあります。

結果

ホスト上のすべてのデータベースが自動的に検出され、[Resources]ページに表示されます。何も表示されない場合は、[リソースの更新] をクリックします。

インストール ステータスの監視

[Jobs]ページを使用して、SnapCenterプラグイン パッケージのインストールの進捗状況を監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、プラグインのインストール操作のみがリストされるようにリストをフィルタリングするには、次の手順を実行します。
 - a. *フィルター*をクリックします。
 - b. オプション：開始日と終了日を指定します。
 - c. [タイプ] ドロップダウン メニューから、[プラグインのインストール] を選択します。

- d. [Status]ドロップダウン メニューから、インストールのステータスを選択します。
 - e. *適用*をクリックします。
4. インストール ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
 5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

LinuxまたはAIX用のプラグイン パッケージをインストールする別の方法

コマンドレットまたはCLIを使用して、Plug-ins Package for LinuxまたはPlug-ins Package for AIXを手動でインストールすることもできます。

プラグインを手動でインストールする前に、`C:\ProgramData\NetApp\SnapCenter\Package Repository`にあるキー **snapcenter_public_key.pub** と **snapcenter_linux_host_plugin.bin.sig** を使用して、バイナリ パッケージの署名を検証する必要があります。



プラグインをインストールするホストに **OpenSSL 1.0.2g** がインストールされていることを確認してください。

次のコマンドを実行して、バイナリ パッケージの署名を検証します。

- Linux ホストの場合: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- AIX ホストの場合: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_aix_host_plugin.bsx.sig snapcenter_aix_host_plugin.bsx`

コマンドレットを使用した複数のリモート ホストへのインストール

複数のホストに Linux 用のSnapCenterプラグイン パッケージまたは AIX 用のSnapCenterプラグイン パッケージをインストールするには、*Install-SmHostPackage* PowerShell コマンドレットを使用する必要があります。

必要なもの

プラグイン パッケージをインストールする各ホストに対するローカル管理者権限を持つドメイン ユーザとして、SnapCenterにログインする必要があります。

手順

1. PowerShellを起動します。
2. SnapCenter Server ホストで、*Open-SmConnection* コマンドレットを使用してセッションを確立し、資格情報を入力します。
3. *Install-SmHostPackage* コマンドレットと必要なパラメータを使用して、Linux 用のSnapCenterプラグイン パッケージまたは AIX 用のSnapCenterプラグイン パッケージをインストールします。

プラグインを既に手動でインストールしていて、ホストがプラグインをインストールするための要件を満たしているかどうかを検証したくない場合は、`-skipprecheck` オプションを使用できます。



事前確認スクリプトでは、ファイアウォールの拒否ルールに指定されているプラグイン ポートのファイアウォール ステータスは検証されません。

4. リモート インストールのクレデンシャルを入力します。

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

クラスタ ホストへのインストール

SnapCenter Plug-ins Package for LinuxまたはSnapCenter Plug-ins Package for AIXは、クラスタ ホストの両方のノードにインストールする必要があります。

クラスタ ホストの各ノードには2つのIPがあります。1つ目は各ノードのパブリックIPで、2つ目は両方のノード間で共有されるクラスタIPです。

手順

1. クラスタ ホストの両方のノードにSnapCenter Plug-ins Package for LinuxまたはSnapCenter Plug-ins Package for AIXをインストールします。
2. `/var/opt/snapcenter/spl/etc/`にある `spl.properties` ファイルで、`SNAPCENTER_SERVER_HOST`、`SPL_PORT`、`SNAPCENTER_SERVER_PORT`、および `SPL_ENABLED_PLUGINS` パラメータの正しい値が指定されていることを確認します。

`spl.properties`に`SPL_ENABLED_PLUGINS`が指定されていない場合は、このパラメータを追加して値SCO,SCUを割り当てることができます。

3. SnapCenter Server ホストで、*Open-SmConnection* コマンドレットを使用してセッションを確立し、資格情報を入力します。
4. 各ノードで、*Set-PreferredHostIPsInStorageExportPolicy* `sccli` コマンドと必要なパラメータを使用して、ノードの優先 IP を設定します。
5. SnapCenter Server ホストで、`C:\Windows\System32\drivers\etc\hosts` にクラスター IP と対応する DNS 名のエントリを追加します。
6. ホスト名のクラスター IP を指定して、*Add-SmHost* コマンドレットを使用してノードをSnapCenter Server に追加します。

ノード1でOracleデータベースを検出し（クラスタIPがノード1でホストされている場合）、データベースのバックアップを作成します。フェイルオーバーが発生した場合は、ノード1に作成されたバックアップを使用してノード2にデータベースをリストアできます。ノード1に作成されたバックアップを使用して、ノード2にクローンを作成することもできます。



他のSnapCenterの処理の実行中にフェイルオーバーが発生した場合は、古いボリューム、ディレクトリ、およびロック ファイルが存在します。

サイレント モードでの**Plug-ins Package for Linux**のインストール

コマンドライン インターフェイス（CLI）を使用して、SnapCenter Plug-ins Package for Linuxをサイレントモードでインストールできます。

必要なもの

- プラグイン パッケージのインストールに必要な前提条件を確認しておく必要があります。
- DISPLAY環境変数が設定されていないことを確認する必要があります。

DISPLAY環境変数が設定されている場合は、unset DISPLAYを実行してからプラグインを手動でインストールする必要があります。

このタスクについて

コンソール モードではインストール中に必要なインストール情報を指定する必要がありますが、サイレントモードでは指定する必要はありません。

手順

1. SnapCenter Serverのインストール先からSnapCenter Plug-ins Package for Linuxをダウンロードします。

デフォルトのインストール パスは `C:\ProgramData\NetApp\SnapCenter\PackageRepository` です。このパスには、SnapCenter Serverがインストールされているホストからアクセスできます。

2. コマンド プロンプトから、インストール ファイルをダウンロードしたディレクトリに移動します。
3. 次のコマンドを実行します。

```
./SnapCenter_linux_host_plugin.bin -i silent-DPORT=8145-  
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-  
DUSER_INSTALL_DIR==/opt/custom_path
```

4. `/var/opt/snapcenter/spl/etc/` にある `spl.properties` ファイルを編集して
`SPL_ENABLED_PLUGINS=SCO,SCU` を追加し、SnapCenter Plug-in Loaderサービスを再起動します。



プラグイン パッケージをインストールすると、SnapCenter Serverではなくホストにプラグインが登録されます。SnapCenter Serverにプラグインを登録するには、SnapCenter GUIまたはPowerShellコマンドレットを使用してホストを追加する必要があります。ホストの追加時にクレデンシャルとして[None]を選択します。ホストを追加すると、インストールしたプラグインが自動的に検出されます。

サイレント モードでのPlug-ins Package for AIXのインストール

コマンドライン インターフェイス (CLI) を使用して、SnapCenter Plug-ins Package for AIXをサイレント モードでインストールできます。

必要なもの

- プラグイン パッケージのインストールに必要な前提条件を確認しておく必要があります。
- DISPLAY環境変数が設定されていないことを確認する必要があります。

DISPLAY環境変数が設定されている場合は、unset DISPLAYを実行してからプラグインを手動でインストールする必要があります。

手順

1. SnapCenter Serverのインストール先からSnapCenter Plug-ins Package for AIXをダウンロードします。

デフォルトのインストール パスは `C:\ProgramData\NetApp\ SnapCenter\PackageRepository` です。このパスには、SnapCenter Serverがインストールされているホストからアクセスできます。

2. コマンド プロンプトから、インストール ファイルをダウンロードしたディレクトリに移動します。
3. 次のコマンドを実行します。

```
./snapcenter_aix_host_plugin.bsx-i silent-DPORT=8145-  
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-  
DUSER_INSTALL_DIR==/opt/custom_path-  
DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-  
DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user
```

4. `/var/opt/snapcenter/spl/etc/` にある `spl.properties` ファイルを編集して
`SPL_ENABLED_PLUGINS=SCO,SCU` を追加し、 SnapCenter Plug-in Loaderサービスを再起動します。



プラグイン パッケージをインストールすると、SnapCenter Serverではなくホストにプラグインが登録されます。SnapCenter Serverにプラグインを登録するには、SnapCenter GUIまたはPowerShellコマンドレットを使用してホストを追加する必要があります。ホストの追加時にクレデンシャルとして[None]を選択します。ホストを追加すると、インストールしたプラグインが自動的に検出されます。

SnapCenter Plug-in Loaderサービスの設定

SnapCenter Plug-in Loaderサービスは、SnapCenter Serverと連動するためにLinuxまたはAIX用のプラグイン パッケージをロードします。SnapCenter Plug-in Loaderサービスは、SnapCenter Plug-ins Package for LinuxまたはSnapCenter Plug-ins Package for AIXのインストール時にインストールされます。

このタスクについて

SnapCenter Plug-ins Package for LinuxまたはSnapCenter Plug-ins Package for AIXのインストール後に、SnapCenter Plug-in Loaderサービスが自動的に開始されます。SnapCenter Plug-in Loaderサービスが自動的に開始されない場合は、次の作業を行う必要があります。

- プラグインが動作しているディレクトリが削除されていないことを確認します。
- Java仮想マシンに割り当てられているメモリ容量を増やします。

`/custom_location/ NetApp/snapcenter/spl/etc/` にある `spl.properties` ファイルには、次のパラメータが含まれています。これらのパラメータにはデフォルト値が割り当てられています。

パラメータ名	説明
LOG_LEVEL	サポートされるログ レベルを表示します。 有効な値は、TRACE、DEBUG、INFO、WARN、ERROR、およびFATALです。

パラメータ名	説明
SPL_PROTOCOL	SnapCenter Plug-in Loaderでサポートされるプロトコルを表示します。 HTTPSプロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。
SNAPCENTER_SERVER_PROTOCOL	SnapCenter Serverでサポートされるプロトコルを表示します。 HTTPSプロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。
SKIP_JAVAHOME_UPDATE	SPLサービスはデフォルトでjavaパスを検出し、JAVA_HOMEパラメータを更新します。 したがって、デフォルト値はFALSEに設定されます。デフォルトの動作を無効にしてjavaパスを手動で修正するには、TRUEに設定します。
SPL_KEYSTORE_PASS	キーストア ファイルのパスワードを表示します。 この値は、パスワードを変更する場合や新しいキーストア ファイルを作成する場合にのみ変更できます。
SPL_PORT	SnapCenter Plug-in Loaderサービスが実行されているポート番号を表示します。 デフォルト値がない場合は、値を追加できます。  プラグインのインストール後に値を変更しないでください。
SNAPCENTER_SERVER_HOST	SnapCenter ServerのIPアドレスまたはホスト名を表示します。
SPL_KEYSTORE_PATH	キーストア ファイルの絶対パスを表示します。
SNAPCENTER_SERVER_PORT	SnapCenter Serverが実行されているポート番号を表示します。

パラメータ名	説明
LOGS_MAX_COUNT	/custom_location/snapcenter/spl/logs フォルダに保存されているSnapCenterプラグLoaderログ ファイルの数を表示します。 デフォルト値は5000に設定されています。この数が指定した値より大きい場合は、最後に変更されたものから5,000個のファイルが保持されます。ファイル数のチェックは、SnapCenter Plug-in Loaderサービスが開始された時点から24時間ごとに自動的行われます。  spl.properties ファイルを手動で削除する場合、保持されるファイル数は9999に設定されます。
JAVA_HOME	SPLサービスの開始に使用されるJAVA_HOMEディレクトリの絶対パスを表示します。 このパスは、インストール時にSPLを開始する段階で決定されます。
LOG_MAX_SIZE	ジョブ ログ ファイルの最大サイズを表示します。 最大サイズに達すると、そのログ ファイルはzipされ、そのジョブの新しいファイルにログが書き込まれます。
RETAIN_LOGS_OF_LAST_DAYS	ログが保持される最大日数が表示されます。
ENABLE_CERTIFICATE_VALIDATION	ホストでCA証明書の検証が有効になっている場合はtrueと表示されます。 このパラメータを有効または無効にするには、spl.propertiesを編集するか、SnapCenterのGUIまたはコマンドレットを使用します。

これらのパラメータにデフォルト値が割り当てられていない場合や、値を割り当てたり変更したりする場合は、spl.propertiesファイルを変更できます。パラメータに割り当てられている値に関連する問題をトラブルシューティングするために、spl.propertiesファイルを検証および編集することもできます。spl.propertiesファイルを変更したら、SnapCenter Plug-in Loaderサービスを再起動する必要があります。

手順

- 必要に応じて、次のいずれかの操作を実行します。
 - SnapCenterプラグインLoaderサービスを開始します。
 - ルートユーザーとして、次を実行します:

```
/custom_location/NetApp/snapcenter/spl/bin/spl start
```

- 非ルートユーザーとして、次を実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
- SnapCenterプラグインLoaderサービスを停止します。
 - ルートユーザーとして、次を実行します: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
 - 非ルートユーザーとして、次を実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`



stopコマンドで-forceオプションを使用すると、SnapCenter Plug-in Loaderサービスを強制的に停止できます。ただし、既存の処理も終了してしまうため、このコマンドを使用する際は十分に注意してください。

- SnapCenterプラグインLoaderサービスを再起動します。
 - ルートユーザーとして、次を実行します: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
 - 非ルートユーザーとして、次を実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
- SnapCenterプラグインLoaderサービスのステータスを確認します。
 - ルートユーザーとして、次を実行します: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
 - 非ルートユーザーとして、次を実行します: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
- SnapCenterプラグインLoaderサービスの変更を見つけます。
 - ルートユーザーとして、次を実行します: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
 - 非ルートユーザーとして、次を実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

LinuxホストでのSnapCenter Plug-in Loader (SPL) サービスを使用したCA証明書の設定

インストールされたデジタル証明書をアクティブ化するには、SnapCenterプラグインLoaderサービスを使用して、SPL キーストアとその証明書のパスワードを管理し、CA 証明書を構成し、SPL 信頼ストアにルート証明書または中間証明書を構成し、CA 署名キー ペアを SPL 信頼ストアに構成する必要があります。



SPLでは、「/var/opt/snapcenter/spl/etc」にある「keystore.jks」ファイルを、トラストストアとキーストアのどちらにも使用します。

SPLキーストアのパスワードと、使用中のCA署名キー ペアのエイリアスの管理

手順

1. SPLキーストアのデフォルト パスワードは、SPLプロパティ ファイルから取得できます。

これは、キー「SPL_KEYSTORE_PASS」に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```

・ キーストア内の秘密キー
エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

spl.propertiesファイルのキーSPL_KEYSTORE_PASSについても、同様に更新します。

3. パスワードを変更したら、サービスを再起動します。



SPLキーストアのパスワードと、秘密キーに関連付けられているエイリアス パスワードをすべて同じにする必要があります。

ルート証明書または中間証明書のSPLトラストストアへの設定

ルート証明書や中間証明書は、SPLトラストストアへの秘密キーなしで設定する必要があります。

手順

1. SPL キーストアが格納されているフォルダー (/var/opt/snapcenter/spl/etc) に移動します。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

・ ルート証明書か中間証明書を追加します。

```
keytool -import -trustcacerts -alias  
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore  
keystore.jks
```

・
SPLトラストストアへのルート証明書または中間証明書を設定したら、サービスを再起動します。
。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

SPLトラストストアに対するCA署名付きキー ペアの設定

SPLトラストストアに対してCA署名付きキー ペアを設定する必要があります。

手順

1. SPLキーストアが格納されているフォルダに移動します：/var/opt/snapcenter/spl/etc
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

- ・ 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore <CertificatePathToImport>  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

- ・ キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

- ・ キーストアに追加された新しい
CA証明書に対応するエイリアスが、キーストアに含まれていることを確認します。
- ・ CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

SPLキーストアのデフォルトのパスワードは、spl.propertiesファイルのキーSPL_KEYSTORE_PASSの値です。

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore  
keystore.jks
```

- ・ CA 証明書のエイリアス名が長く、スペースや特殊文字（「*」、「」）
が含まれている場合は、エイリアス名を単純な名前に変更します。

```
keytool -changealias -alias "<OriginalAliasName>" -destalias  
"<NewAliasName>" -keystore keystore.jks
```

- ・ spl.propertiesファイルにあるキーストアからエイリアス名を設定します。

SPL_CERTIFICATE_ALIASキーに対するこの値を更新します。

4. SPLトラストストアにCA署名キー ペアを設定したら、サービスを再起動します。

SPLの証明書失効リスト（CRL）の設定

SPLにCRLを設定する必要があります。

このタスクについて

- SPLは、あらかじめ設定されたディレクトリでCRLファイルを検索します。
- SPL の CRL ファイルのデフォルト ディレクトリは `/var/opt/snapcenter/spl/etc/crl` です。

手順

1. キーSPL_CRL_PATHに照らしてspl.propertiesファイルのデフォルト ディレクトリを変更および更新できます。
2. このディレクトリには、複数のCRLファイルを格納できます。

受信する証明書については、それぞれのCRLに対して検証が行われます。

プラグインのCA証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインでCA証明書の検証を有効にする必要があります。

開始する前に

- 実行 `Set-SmCertificateSettings` コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- `Get-SmCertificateSettings` を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで使えるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. プラグイン ホストを1つまたは複数選択します。
4. *その他のオプション*をクリックします。
5. *証明書の検証を有効にする*を選択します。

終了後の操作

[Managed Hosts]タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Serverとプラグイン ホスト間の接続のステータスを示します。

- *🔑* は、CA 証明書が有効になっていないか、プラグイン ホストに割り当てられていないことを示します。
- *🟢* は CA 証明書が正常に検証されたことを示します。
- *🔴* は、CA 証明書を検証できなかったことを示します。
- *🔒* は接続情報を取得できなかったことを示します。



ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

SnapManager for OracleおよびSnapManager for SAPからのSnapCenterへのデータのインポート

SnapManager for OracleとSnapManager for SAPからSnapCenterにデータをインポートすると、以前のバージョンのデータを引き続き使用できるようになります。

SnapManager for OracleおよびSnapManager for SAPからSnapCenterにデータをインポートするには、コマンドライン インターフェイス（LinuxホストのCLI） からインポート ツールを実行します。

インポート ツールを実行すると、SnapCenterでポリシーとリソース グループが作成されます。SnapCenterで作成されるポリシーとリソース グループは、SnapManager for OracleおよびSnapManager for SAPのプロファイルとそれらのプロファイルを使用して実行される処理に対応します。SnapCenterのインポート ツールで処理の対象となるのは、SnapManager for OracleおよびSnapManager for SAPのリポジトリ データベースとインポート対象のデータベースです。

- すべてのプロファイル、スケジュール、およびプロファイルを使用して実行される処理が取得されます。
- 一意の処理ごと、およびプロファイルに関連付けられているスケジュールごとに、SnapCenterのバックアップ ポリシーが作成されます。
- ターゲット データベースごとにリソース グループが作成されます。

`/opt/ NetApp/snapcenter/spl/bin` にある `sc-migrate` スクリプトを実行することで、インポート ツールを実行できます。インポートするデータベース ホストに Linux 用のSnapCenterプラグイン パッケージをインストールすると、`sc-migrate` スクリプトが `/opt/ NetApp/snapcenter/spl/bin` にコピーされます。



データのインポートは、SnapCenterのグラフィカル ユーザ インターフェイス（GUI）ではサポートされていません。

SnapCenterでは、Data ONTAP 7-Modeはサポートされていません。7-Mode Transition Toolを使用すると、Data ONTAP 7-Modeを実行しているシステムに保存されたデータと設定をONTAPシステムに移行できます。

データのインポートがサポートされる構成

SnapManager 3.4.x for OracleおよびSnapManager 3.4.x for SAPからSnapCenterにデータをインポートする前に、SnapCenter Plug-in for Oracle Databaseでサポートされる構成を確認しておく必要があります。

SnapCenter Plug-in for Oracle Databaseでサポートされている構成は、["NetApp Interoperability Matrix Tool"](#)。

SnapCenterにインポートされるデータ

プロファイル、スケジュール、およびプロファイルを使用して実行する処理をインポートできます。

SnapManager for OracleおよびSnapManager for SAP	SnapCenter
処理とスケジュールが設定されていないプロファイル	デフォルトの設定（バックアップ タイプが「オンライン」でバックアップの範囲が「フル」）でポリシーが作成されます。

SnapManager for OracleおよびSnapManager for SAP	SnapCenter
1つ以上の処理が設定されたプロファイル	プロファイルとそのプロファイルを使用して実行される処理の一意の組み合わせに基づいて複数のポリシーが作成されます。 SnapCenterで作成されるポリシーには、プロファイルおよび対応する処理から取得されたアーカイブ ログの削除と保持の詳細が含まれます。
Oracle Recovery Manager (RMAN) の設定を含むプロファイル	ポリシーは、Oracle Recovery Manager を使用したカタログ バックアップ オプションを有効にして作成されます。 SnapManagerで外部のRMANのカタログ化を使用していた場合は、SnapCenterでRMANカタログの設定を行う必要があります。既存のクレデンシャルを選択するか、新しいクレデンシャルを作成できます。 SnapManagerで制御ファイルを使用してRMANを設定していた場合は、SnapCenterでRMANの設定を行う必要はありません。
プロファイルに関連付けられているスケジュール	スケジュールに対して専用のポリシーが作成されます。
データベース	インポートしたデータベースごとにリソース グループが作成されます。 Real Application Cluster (RAC) セットアップでは、インポート後にインポート ツールを実行したノードが優先ノードになり、そのノードに対してリソースグループが作成されます。



プロファイルのインポート時は、バックアップ ポリシーと一緒に検証ポリシーが作成されます。

SnapManager for OracleとSnapManager for SAPのプロファイル、スケジュール、およびプロファイルを使用して実行される処理をSnapCenterにインポートすると、異なるパラメータの値もインポートされます。

SnapManager for Oracle およびSnapManager for SAPのパラメータと値	SnapCenterのパラメータと値	注記
バックアップ対象 • 満杯 • データ • ログ	バックアップ対象 • 満杯 • データ • ログ	
バックアップ モード • Auto • オンライン • オフライン	バックアップ タイプ • オンライン • オフラインシャットダウン	バックアップ モードが自動の場合、インポート ツールは操作の実行時にデータベースの状態を確認し、バックアップ タイプをオンラインまたはオフライン シャットダウンのいずれかに適切に設定します。
保持 • Days • Counts	保持 • Days • Counts	SnapManager for Oracle とSnapManager for SAPでは、[Days]と[Counts]の両方を使用して保持が設定されます。 SnapCenterには、日数またはカウントのいずれかがあります。SnapManager for Oracle とSnapManager for SAPで個数よりも日数が優先されるため、保持は日数に基づいて設定されます。
スケジュールの削除 • All • System Change Number (SCN) • Date • Logs created before specified hours, days, weeks, and months	スケジュールの削除 • All • 指定された時間と日の前に作成されたログ	SnapCenterでは、SCN、日付、および週と月の数に基づく削除はサポートされていません。
通知 • 成功した操作に対してのみメールを送信します • 失敗した操作についてのみメールを送信 • 成功した操作と失敗した操作の両方について送信されるメール	通知 • いつも • 失敗した場合 • 警告 • エラー	Eメール通知はインポートの対象になります。 ただし、SnapCenterのGUIを使用してSMTPサーバを手動で更新する必要があります。Eメールの件名は、設定できるように空白になります。

SnapCenterにインポートされないデータ

インポート ツールによって、すべてのデータがSnapCenterにインポートされるわけではありません。

次のデータはSnapCenterにインポートできません。

- バックアップ メタデータ
- 部分バックアップ
- rawデバイス マッピング (RDM) およびVirtual Storage Console (VSC) 関連のバックアップ
- SnapManager for OracleおよびSnapManager for SAPのリポジトリで使用可能なロールとクレデンシヤル
- 検証、リストア、クローニングの処理に関するデータ
- 処理の削除
- SnapManager for OracleおよびSnapManager for SAPのプロファイルで指定されたレプリケーションの詳細

インポートの完了後に、SnapCenterで作成した対応するポリシーを手動で編集してレプリケーションの詳細を含める必要があります。

- カタログ化されたバックアップの情報

データのインポートの準備

SnapCenterへのデータのインポート処理を正常に実行するには、データをインポートする前に一定のタスクを実行しておく必要があります。

手順

1. インポートするデータベースを特定します。
2. SnapCenterを使用してデータベース ホストを追加し、SnapCenter Plug-ins Package for Linuxをインストールします。
3. SnapCenterを使用して、ホストのデータベースで使用されるStorage Virtual Machine (SVM) の接続をセットアップします。
4. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
5. [Resources] ページで、インポートするデータベースが検出されて表示されていることを確認します。

インポート ツールを実行する場合は、データベースにアクセスできる必要があります。アクセスできないと、リソース グループの作成が失敗します。

データベースでクレデンシヤルが設定されている場合は、対応するクレデンシヤルをSnapCenterで作成し、そのクレデンシヤルをデータベースに割り当ててから、データベースの検出を再度実行する必要があります。データベースがAutomatic Storage Management (ASM) にある場合は、ASMインスタンスのクレデンシヤルを作成し、そのクレデンシヤルをデータベースに割り当てる必要があります。

6. インポート ツールを実行するユーザに、SnapManager for OracleまたはSnapManager for SAPのホストからSnapManager for OracleまたはSnapManager for SAPのCLIコマンド（スケジュールを中断するコマンドなど）を実行するための十分な権限があることを確認します。
7. SnapManager for OracleまたはSnapManager for SAPのホストで、次のコマンドを実行してスケジュール

を中断します。

a. SnapManager for Oracleホストでスケジュールを一時停止する場合は、次のコマンドを実行します。

- `smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
- `smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smo credential set -profile -name profile_name`



smo credential setコマンドは、ホストの各プロファイルに対して実行する必要があります。

b. SnapManager for SAPホストでスケジュールを一時停止する場合は、次のコマンドを実行します。

- `smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
- `smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smsap credential set -profile -name profile_name`



smsap credential setコマンドは、ホストの各プロファイルに対して実行する必要があります。

8. `hostname -f`を実行して、データベース ホストのFully Qualified Domain Name (FQDN;完全修飾ドメイン名)が表示されることを確認します。

FQDNが表示されない場合は、`/etc/hosts`を変更してホストのFQDNを指定する必要があります。

データのインポート

データベース ホストからインポート ツールを実行してデータをインポートすることができます。

このタスクについて

インポート後にSnapCenterで作成されるバックアップ ポリシーの名前の形式は、対象に応じて次のように異なります。

- 処理とスケジュールが設定されていないプロファイルに対しては、`SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED`の形式でポリシーが作成されます。

プロファイルを使用して実行される処理がない場合、そのプロファイルについてはデフォルトの設定（バックアップ タイプがオンラインでバックアップの範囲がフル）で対応するポリシーが作成されます。

- 1つ以上の処理が設定されたプロファイルに対しては、`SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED`の形式でポリシーが作成されます。

- プロファイルに関連付けられているスケジュールに対しては、SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATEDの形式でポリシーが作成されます。

手順

1. インポートするデータベース ホストにログインします。
2. `/opt/NetApp/snapcenter/spl/bin` にある `sc-migrate` スクリプトを実行して、インポート ツールを実行します。
3. SnapCenter Serverのユーザ名とパスワードを入力します。

クレデンシャルの検証後、SnapCenterとの接続が確立されます。

4. SnapManager for OracleまたはSnapManager for SAPのリポジトリ データベースの詳細を入力します。

リポジトリ データベースのホストで使用可能なデータベースが表示されます。

5. ターゲット データベースの詳細を入力します。

ホストのすべてのデータベースをインポートする場合は、「all」と入力します。

6. 失敗した操作についてシステム ログを生成したり、ASUP メッセージを送信したりする場合は、`Add-SmStorageConnection` コマンドまたは `Set-SmStorageConnection` コマンドを実行してそれらを有効にする必要があります。



インポート処理をキャンセルする場合、インポート ツールの実行中またはインポートの完了後に、インポート処理で作成されたSnapCenterポリシー、クレデンシャル、およびリソース グループを手動で削除する必要があります。

結果

プロファイル、スケジュール、およびプロファイルを使用して実行される処理に対応するSnapCenterのバックアップ ポリシーが作成されます。また、各ターゲット データベースに対応するリソース グループも作成されます。

データのインポートが正常に完了すると、SnapManager for OracleおよびSnapManager for SAPで、インポートしたデータベースに関連付けられたスケジュールが中断されます。



インポートの完了後は、インポートしたデータベースまたはファイルシステムをSnapCenterで管理する必要があります。

インポート ツールの実行ごとのログは、`spl_migration_timestamp.log` という名前で `/var/opt/snapcenter/spl/logs` ディレクトリに保存されます。このログでインポート エラーを確認し、トラブルシューティングを行うことができます。

SnapCenter Plug-in for VMware vSphereのインストール

データベースまたはファイルシステムが仮想マシン（VM）に格納されている場合や、VMとデータストアを保護する場合は、SnapCenter Plug-in for VMware vSphere仮想

アプライアンスを導入する必要があります。

展開方法については、["導入プロセスの概要"](#)。

CA証明書を導入する

SnapCenter Plug-in for VMware vSphereで CA 証明書を構成するには、以下を参照してください。"[SSL証明書を作成またはインポートする](#)"。

CRLファイルを設定する

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリでCRLファイルを探します。SnapCenter Plug-in for VMware vSphere のCRL ファイルのデフォルト ディレクトリは `/opt/netapp/config/crl` です。

このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

Oracleデータベースの保護の準備

バックアップ、クローニング、リストアなどのデータ保護処理を実行する場合は、事前に戦略を定義し、環境をセットアップする必要があります。SnapMirrorテクノロジーとSnapVaultテクノロジーを使用できるようにSnapCenter Serverをセットアップすることもできます。

SnapVaultテクノロジーとSnapMirrorテクノロジーを利用するには、ストレージ デバイス上のソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、初期化する必要があります。この作業を行うには、NetApp System Managerを使用するか、ストレージ コンソールのコマンドラインを使用します。

ユーザがPlug-in for Oracle Databaseを使用するためには、SnapCenter管理者が事前にSnapCenter Serverをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter Server をインストールして構成します。["詳細情報"](#)
- ストレージ システム接続を追加して、 SnapCenter環境を構成します。["詳細情報"](#)



SnapCenterでは、別々のクラスタに属している場合でも、複数のSVMに同じ名前を付けることはサポートされません。SVMの登録またはクラスタの登録を使用してSnapCenterに登録されるSVMは、それぞれ一意である必要があります。

- インストール ユーザーに対して、認証モードを Linux または AIX にして資格情報を作成します。["詳細情報"](#)
- ホストを追加し、プラグインをインストールし、リソースを検出します。
- VMware RDM LUNまたはVMDKにあるOracleデータベースをSnapCenter Serverを使用して保護する場合は、SnapCenter Plug-in for VMware vSphereを導入して、プラグインをSnapCenterに登録する必要があります。
- LinuxホストまたはAIXホストにJavaをインストールします。

見る["Linuxホストの要件"または"AIXホストの要件"](#)詳細についてはこちらをご覧ください。

- アプリケーション ファイアウォールのタイムアウト値は3時間以上に設定する必要があります。
- NFS環境でOracleデータベースを使用している場合は、マウント、クローニング、検証、リストアの各処理を実行できるように、プライマリ ストレージまたはセカンダリ ストレージ用に少なくとも1つのNFSデータLIFを設定しておく必要があります。
- データ パス (LIF) が複数ある場合、またはdNFS構成を使用している場合は、データベース ホストでSnapCenter CLIを使用して次の作業を実行できます。
 - デフォルトでは、データベース ホストのすべての IP アドレスが、クローン ボリュームのストレージ 仮想マシン (SVM) の NFS ストレージ エクスポート ポリシーに追加されます。IPアドレスを1つにするか、一部のIPアドレスに制限する場合は、Set-PreferredHostIPsInStorageExportPolicy CLIを実行します。
 - SVM に複数のデータ パス (LIF) がある場合、SnapCenter はNFS クローン ボリュームをマウントするための適切なデータ パス (LIF) を選択します。ただし、データ パス (LIF) を1つに特定する場合は、Set-SvmPreferredDataPath CLIを実行する必要があります。詳細については、『[コマンド リファレンス ガイド](#)』を参照してください。
- SAN環境でOracleデータベースを使用している場合は、以下のガイドに記載されている推奨事項に従ってSAN環境が設定されていることを確認します。
 - ["ONTAPストレージでLinuxホストを使用する"](#)
 - ["Host Settings Affected by AIX Host Utilities"](#)
- Oracle LinuxまたはRHELオペレーティング システムのLVMでOracleデータベースを使用している場合は、最新バージョンの論理ボリューム マネージャ (LVM) をインストールします。
- SnapManager for Oracleを使用していて、SnapCenter Plug-in for Oracle Databaseに移行する場合は、sccliコマンドsc-migrateを使用して、SnapCenterのポリシーとリソース グループにプロファイルを移行できます。
- バックアップ レプリケーションが必要な場合は、ONTAPでSnapMirrorとSnapVaultを設定します。

SnapCenter Plug-in for VMware vSphere 4.1.1のドキュメントには、SnapCenter 4.1.1のユーザ向けに、仮想データベースとファイルシステムの保護に関する情報が記載されています。NetApp Data Broker 1.0および1.0.1のドキュメントには、SnapCenter 4.2.xのユーザ向けに、LinuxベースのNetApp Data Broker仮想アプライアンス (オープン仮想アプライアンス形式) が提供するSnapCenter Plug-in for VMware vSphereを使用した仮想データベースとファイルシステムの保護に関する情報が記載されています。SnapCenter Plug-in for VMware vSphere 4.3のドキュメントには、SnapCenter 4.3.xのユーザ向けに、LinuxベースのSnapCenter Plug-in for VMware vSphere仮想アプライアンス (オープン仮想アプライアンス形式) を使用した仮想データベースとファイルシステムの保護に関する情報が記載されています。

詳細情報

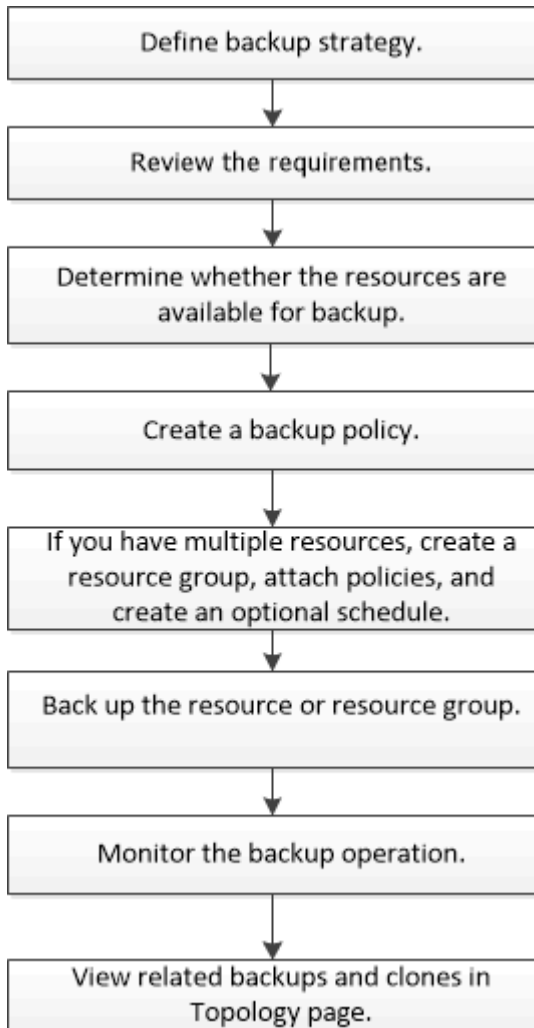
- ["Interoperability Matrix Tool"](#)
- ["SnapCenter Plug-in for VMware vSphereのドキュメント"](#)
- ["RHEL 7以降の非マルチパス環境でデータ保護処理が失敗する"](#)

Oracleデータベースのバックアップ

バックアップ手順の概要

リソース（データベース）またはリソース グループのバックアップを作成することができます。バックアップ手順には、計画、バックアップするリソースの特定、バックアップ ポリシーの作成、リソース グループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

次のワークフローは、バックアップ処理の実行順序を示しています。



Oracle データベースのバックアップを作成する際に、データベース上で複数の操作が実行されないように、Oracle データベース ホストの `/var/opt/snapcenter/sco/lock` ディレクトリに操作ロック ファイル (`.sm_lock_dbsid`) が作成されます。処理ロック ファイルは、データベースのバックアップが完了すると自動的に削除されます。

ただし、前回のバックアップが完了したものの警告が表示された場合は、処理ロック ファイルが削除されず、次のバックアップ処理が待機キューに登録される可能性があります。`.sm_lock_dbsid` ファイルが削除されない場合、最終的にはキャンセルされる可能性があります。そのような場合は、次の手順を実行して、処理ロック ファイルを手動で削除する必要があります。

1. コマンドプロンプトから、`/var/opt/snapcenter/sco/lock` に移動します。
2. 操作ロックを削除します。`rm -rf .sm_lock_dbsid.`

バックアップ構成情報

バックアップ対象としてサポートされる**Oracle**データベース構成

SnapCenterでは、各種のOracleデータベース構成のバックアップがサポートされます。

- Oracle Standalone
- Oracle Real Application Clusters (RAC)
- Oracle Standalone Legacy
- Oracle Standalone Container Database (CDB)
- Oracle Data Guardスタンバイ

Data Guardスタンバイ データベースで作成できるのは、オフライン マウント バックアップのみです。オフライン シャットダウン バックアップ、アーカイブ ログのみのバックアップ、フル バックアップはサポートされていません。

- Oracle Active Data Guardスタンバイ

Active Data Guardスタンバイ データベースで作成できるのは、オンライン バックアップのみです。アーカイブ ログのみのバックアップとフル バックアップはサポートされていません。

Data Guardスタンバイ データベースまたはActive Data Guardスタンバイ データベースのバックアップを作成する場合は、管理されたリカバリ プロセス (MRP) が事前に停止し、バックアップが作成されたあとにMRPが開始されます。

- Automatic Storage Management (ASM)
 - ASM スタンドアロンおよび仮想マシン ディスク (VMDK) 上の ASM RAC

Oracleデータベースでサポートされているすべてのリストア方式の中で、VMDK上のASM RACデータベースで実行できるのはConnect and Copyリストアだけです。
 - ASM スタンドアロンおよび Raw デバイス マッピング (RDM) 上の ASM RAC + ASMLib の有無にかかわらず、ASM 上の Oracle データベースでバックアップ、復元、およびクローン操作を実行できます。
 - Oracle ASMフィルタ ドライバ (ASMFD)

PDB移行およびPDBクローニング処理はサポートされていません。
 - Oracle Flex ASM

サポートされているOracleバージョンの最新情報については、["NetApp Interoperability Matrix Tool"](#)。

Oracleデータベースでサポートされるバックアップ タイプ

バックアップ タイプでは、作成するバックアップのタイプを指定します。SnapCenterでは、Oracleデータベースに対してオンライン バックアップ タイプとオフライン バックアップ タイプがサポートされます。

オンライン バックアップ

データベースがオンライン状態のときに作成されるバックアップを、オンライン バックアップと呼びます。ホット バックアップとも呼ばれるオンライン バックアップでは、データベースをシャットダウンすることなくバックアップを作成できます。

オンライン バックアップでは、次のファイルのバックアップを作成できます。

- データ ファイルと制御ファイルのみ
- アーカイブ ログ ファイルのみ（この場合はデータベースがバックアップ モードになりません）
- データベース全体（データ ファイル、制御ファイル、およびアーカイブ ログ ファイル）

オフライン バックアップ

データベースがマウント済み状態またはシャットダウン状態のときに作成されるバックアップを、オフライン バックアップと呼びます。オフライン バックアップはコールド バックアップとも呼ばれます。オフライン バックアップにはデータ ファイルと制御ファイルのみを含めることができます。オフライン マウント バックアップまたはオフライン シャットダウン バックアップのいずれかを作成できます。

- オフライン マウント バックアップを作成する場合は、データベースがマウント済み状態であることを確認する必要があります。

データベースがそれ以外の状態であると、バックアップ処理は失敗します。

- オフライン シャットダウン バックアップを作成する場合は、データベースはどの状態でもかまいません。

データベースは、バックアップを作成するために必要な状態に変更されます。バックアップが作成されると、データベースは元の状態に戻ります。

SnapCenterのOracleデータベース検出方法

リソースは、SnapCenterによって管理されるホスト上の Oracle データベースです。使用できるデータベースを検出したあとに、それらのデータベースをリソース グループに追加してデータ保護処理を実行できます。

次のセクションでは、さまざまなタイプとバージョンのOracleデータベースを検出するためにSnapCenterが使用するプロセスについて説明します。

Oracle バージョン 11g から 12cR1 の場合

RACデータベース

RAC データベースは、/etc/oratab エントリに基づいてのみ検出されます。/etc/oratabファイルにデータベース エントリが含まれている必要があります。

スタンドアロン

スタンドアロン データベースは、/etc/oratabエントリに基づいてのみ検出されます。

ASM

ASMインスタンス エントリが/etc/oratabファイルに含まれている必要があります。

RAC One Node

RAC One Nodeデータベースは、`/etc/oratab` エントリに基づいてのみ検出されます。データベースは、`nomount`、`mount`、または `open` のいずれかの状態である必要があります。`/etc/oratab` ファイルにデータベース エントリが含まれている必要があります。

データベースがすでに検出され、バックアップがデータベースに関連付けられている場合、RAC One Nodeデータベースのステータスは名前変更または削除とマークされます。

データベースを再配置した場合は、次の手順を実行する必要があります。

1. フェイルオーバーされたRACノードの`/etc/oratab`ファイルに、再配置されたデータベースのエントリを手動で追加します。
2. リソースを手動で更新します。
3. リソース ページから RAC One Node データベースを選択し、「データベース設定」をクリックします。
4. データベースを設定して、データベースを現在ホストしているRACノードに優先クラスタ ノードを設定します。
5. SnapCenterの処理を実行します。
6. あるノードから別のノードにデータベースを再配置したときに、以前のノードの`oratab`エントリが削除されていない場合は、同じデータベースが2回表示されないように、`oratab`エントリを手動で削除します。

Oracleバージョン12cR2から18c、19c、または21cの場合

RACデータベース

RACデータベースは`srvctl config`コマンドを使用して検出されます。`/etc/oratab` ファイルにデータベース エントリが含まれている必要があります。

スタンドアロン

スタンドアロン データベースは、`/etc/oratab` ファイルのエントリと`srvctl config`コマンドの出力に基づいて検出されます。

ASM

ASMインスタンス エントリが`/etc/oratab`ファイルに含まれている必要はありません。

RAC One Node

RAC One Nodeデータベースは、`srvctl config`コマンドのみを使用して検出されます。データベースは、`nomount`、`mount`、または `open` のいずれかの状態である必要があります。データベースがすでに検出され、バックアップがデータベースに関連付けられている場合、RAC One Nodeデータベースのステータスは名前変更または削除とマークされます。

データベースを再配置する場合は、次の手順を実行する必要があります。リソースを手動で更新します。。リソース ページから RAC One Node データベースを選択し、「データベース設定」をクリックします。。データベースを設定して、データベースを現在ホストしているRACノードに優先クラスタ ノードを設定します。。SnapCenterの処理を実行します。



`/etc/oratab` ファイルに Oracle 12cR2 および 18c データベース エントリがあり、同じデータベースが `srvctl config` コマンドで登録されている場合、SnapCenter は重複するデータベース エントリを削除します。古いデータベース エントリがある場合、データベースは検出されますが、データベースは到達不能になり、ステータスはオフラインになります。

RACセットアップにおける優先ノード

Oracle Real Application Clusters (RAC) セットアップでは、SnapCenterがバックアップ操作を実行するために使用する優先ノードを指定できます。優先ノードを指定しない場合は、SnapCenterによって自動的に優先ノードが割り当てられ、そのノードにバックアップが作成されます。

優先ノードには、RACデータベース インスタンスが存在するクラスター ノードを1つまたは複数指定できます。バックアップ処理は、指定したノードでのみ、指定した順序で実行されます。

例

RACデータベースcdbracに3つのインスタンスがあり、cdbrac1はnode1に、cdbrac2はnode2に、cdbrac3はnode3に置かれているとします。

node1とnode2のインスタンスが優先ノードとして設定され、node2に第1優先順位、node1に第2優先順位が指定されています。バックアップ処理を実行すると、まず第1優先ノードであるnode2で処理が試行されます。

node2がバックアップできる状態にない場合（ホストでプラグイン エージェントが実行されていない、ホスト上のデータベース インスタンスが指定したタイプのバックアップを行うのに必要な状態にない、Flex ASM構成のnode2上のデータベース インスタンスがローカルASMインスタンスによって処理されていない、などの複数の原因が考えられます）、node1で処理が試行されます。

node3は、優先ノードのリストに含まれていないため、バックアップには使用されません。

Flex ASMセットアップ

Flex ASMセットアップでは、カーディナリティがRACクラスター内のノード数より少ない場合、リーフ ノードは優先ノードとしてリストされません。Flex ASMクラスター ノードのロールに変更があった場合は、優先ノードが更新されるように手動で検出する必要があります。

必要なデータベースの状態

バックアップを正常に完了するには、優先ノード上のRACデータベース インスタンスが必要な状態であることが必要です。

- オンライン バックアップを作成する場合は、設定された優先ノードのRACデータベース インスタンスの1つがオープン状態であることが必要です。
- オフライン マウント バックアップを作成する場合は、設定された優先ノードのRACデータベース インスタンスの1つがマウント状態であり、かつ他の優先ノードを含むその他すべてのインスタンスがマウント状態またはそれより低いレベルの状態であることが必要です。
- オフライン シャットダウン バックアップを作成する場合は、RACデータベース インスタンスはどの状態でもかまいませんが、優先ノードを指定する必要があります。

Oracle Recovery Managerを使用してバックアップをカタログ化する方法

Oracle Recovery Manager (RMAN) でOracleデータベースのバックアップをカタログ化することにより、Oracle RMANリポジトリにバックアップ情報を保存できます。

カタログ化されたバックアップは、あとからブロックレベルのリストア処理や表領域のポイントインタイムリカバリ処理に使用できます。カタログ化されたバックアップが不要となった場合は、カタログ情報を削除で

きます。

カタログ化するためには、データベースの状態が少なくともマウント済み状態であることが必要です。カタログ化を実行できるのは、データ バックアップ、アーカイブ ログ バックアップ、およびフル バックアップです。複数のデータベースを含むリソース グループのバックアップに対してカタログ化を有効にすると、データベースごとにカタログ化が実行されます。Oracle RACデータベースの場合は、データベースが少なくともマウント済み状態になっている優先ノードでカタログ化が実行されます。

RACデータベースのバックアップをカタログ化する場合は、そのデータベースに対して他のジョブが実行されていないことを確認します。別のジョブが実行されている場合は、カタログ化処理がキューに登録されずに失敗します。

外部カタログ データベース

デフォルトでは、ターゲット データベースの制御ファイルがカタログ化に使用されます。外部カタログ データベースを追加する場合は、SnapCenterグラフィカル ユーザ インターフェイス (GUI) から[Database Settings]ウィザードを使用して外部カタログのクレデンシャルとTransparent Network Substrate (TNS) 名を指定することにより、そのデータベースを設定できます。外部カタログ データベースはCLIから設定することもできます。その場合は、Configure-SmOracleDatabaseコマンドを、-OracleRmanCatalogCredentialNameオプションおよび-OracleRmanCatalogTnsNameオプションとともに実行します。

RMANコマンド

SnapCenter GUIでOracleバックアップ ポリシーを作成する際にカタログ化オプションを有効にした場合は、バックアップ処理の一環としてOracle RMANを使用してバックアップがカタログ化されます。バックアップの遅延カタログ作成を実行するには、`Catalog-SmBackupWithOracleRMAN`指示。

バックアップをカタログ化した後、`Get-SmBackupDetails`カタログ化されたデータファイルのタグ、制御ファイルのカタログパス、カタログ化されたアーカイブ ログの場所などのカタログ化されたバックアップ情報を取得するコマンド。

命名形式

SnapCenter 3.0では、ASMディスク グループ名が16文字以上である場合に、バックアップに対してSC_HASHCODEofDISKGROUP_DBSID_BACKUPIDという命名形式が使用されます。一方、ディスク グループ名が16文字未満である場合は、バックアップに対してDISKGROUPNAME_DBSID_BACKUPIDという命名形式が使用されます。これはSnapCenter 2.0で使用される形式と同じです。

HASHCODEofDISKGROUPは自動生成される2～10桁の番号で、各ASMディスク グループに固有です。

クロスチェック処理

バックアップに関するRMANリポジトリ情報が古くなってバックアップのリポジトリ レコードがその物理ステータスと一致しなくなった場合は、クロスチェックを実行してリポジトリ情報を更新できます。たとえば、ユーザがオペレーティング システム コマンドでディスクからアーカイブ ログを削除した場合、実際にはディスクにログがないにもかかわらず、制御ファイルにはディスクにログがあることが示されます。

クロスチェック処理では、制御ファイルの情報を更新できます。クロスチェックを有効にするには、Set-SmConfigSettingsコマンドを実行し、ENABLE_CROSSCHECKパラメータにTRUEを割り当てます。デフォルト値はFALSEです。

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings  
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

カタログ情報の削除

カタログ情報を削除するには、Uncatalog-SmBackupWithOracleRMANコマンドを実行します。SnapCenter GUIではカタログ情報を削除できません。ただし、バックアップを削除するとき、またはカタログ化されたバックアップに関連する保持設定とリソース グループを削除するときに、カタログ化されたバックアップの情報も削除されます。



SnapCenterホストを強制的に削除する場合は、そのホストに関連するカタログ化されたバックアップの情報が削除されません。ホストを強制的に削除する場合は、事前にそのホストに関連するすべてのカタログ化されたバックアップの情報を削除しておく必要があります。

処理時間がORACLE_PLUGIN_RMAN_CATALOG_TIMEOUTパラメータに指定されたタイムアウト値を超えたためにカタログ化やカタログ化解除が失敗した場合は、次のコマンドを実行してパラメータの値を変更する必要があります。

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType  
Plugin -PluginCode SCO-ConfigSettings  
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

パラメータの値を変更したら、次のコマンドを実行してSnapCenter Plug-in Loader (SPL) サービスを再起動します。

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

コマンドで利用できるパラメータとその説明は、Get-Help command_nameを実行して確認できます。または、"[SnapCenterソフトウェア コマンド リファレンス ガイド](#)"。

バックアップ固有のプリスクリプトとポストスクリプト用に事前定義された環境変数

SnapCenterでは、バックアップ ポリシーの作成時にプリスクリプトとポストスクリプトを実行する際に、事前定義された環境変数を使用できます。この機能は、VMDKを除くすべてのOracle設定でサポートされます。

SnapCenterにより、シェル スクリプトが実行される環境で直接アクセスできるパラメータの値が事前に定義されます。スクリプトの実行時に、これらのパラメータの値を手動で指定する必要はありません。

バックアップ ポリシーの作成でサポートされる事前定義された環境変数

- **SC_JOB_ID** は操作のジョブ ID を指定します。

例: 256

- **SC_ORACLE_SID** はデータベースのシステム識別子を指定します。

複数のデータベースが処理対象となる場合、パラメータにはパイプで区切られたデータベース名が含まれます。

このパラメータはアプリケーション ボリュームに対して設定されます。

例: NFSB32|NFSB31

- **SC_HOST** はデータベースのホスト名を指定します。

RACの場合、ホスト名はバックアップが実行されるホストの名前です。

このパラメータはアプリケーション ボリュームに対して設定されます。

例: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** は、データベースのオペレーティング システムの所有者を指定します。

データは <db1>@<osuser1>|<db2>@<osuser2> の形式になります。

例: NFSB31@oracle|NFSB32@oracle

- **SC_OS_GROUP** は、データベースのオペレーティング システム グループを指定します。

データは <db1>@<osgroup1>|<db2>@<osgroup2> の形式になります。

例: NFSB31@install|NFSB32@oinstall

- **SC_BACKUP_TYPE** は、バックアップの種類（オンラインフル、オンラインデータ、オンラインログ、オフラインシャットダウン、オフラインマウント）を指定します。

例:

- 完全バックアップの場合: ONLINEFULL
- データのみのバックアップ: ONLINEDATA
- ログのみのバックアップの場合: ONLINELOG

- **SC_BACKUP_NAME** はバックアップの名前を指定します。

このパラメータはアプリケーション ボリュームに対して設定されます。

例: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1|AV@RG2_scspr2417819002_07-20-2021_12.16.48.9267

- **SC_BACKUP_ID** はバックアップ ID を指定します。

このパラメータはアプリケーション ボリュームに対して設定されます。

例: DATA@203|LOG@205|AV@207

- **SC_ORACLE_HOME** は、Oracle ホーム ディレクトリのパスを指定します。

例: NFSB32@/ora01/app/oracle/product/18.1.0/db_1|NFSB31@/ora01/app/oracle/product/18.1.0/db_1

- **SC_BACKUP_RETENTION** は、ポリシーで定義された保持期間を指定します。

例:

- 完全バックアップの場合: 毎時|DATA@DAYS:3|LOG@COUNT:4
- オンデマンドデータのみのバックアップの場合: Ondemand|DATA@COUNT:2
- オンデマンドログのみのバックアップの場合: Ondemand|LOG@COUNT:2

- **SC_RESOURCE_GROUP_NAME** はリソース グループの名前を指定します。

例：RG1

- **SC_BACKUP_POLICY_NAME** は、バックアップ ポリシーの名前を指定します。

例：backup_policy

- **SC_AV_NAME** はアプリケーション ボリュームの名前を指定します。

例：AV1|AV2

- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** は、データ ファイル ディレクトリのボリュームへの SVM のストレージ マッピングを指定します。LUNおよびqtreeの親ボリュームの名前になります。

データは <db1>@<SVM1:volume1>|<db2>@<SVM2:volume2> としてフォーマットされます。

例:

- 同じリソース グループ内の 2 つのデータベースの場合:
NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA
- データ ファイルが複数のボリュームに分散している単一のデータベースの場合
: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_NFS
- **SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH** は、ログ ファイル ディレクトリのボリュームへの SVM のストレージ マッピングを指定します。LUNおよびqtreeの親ボリュームの名前になります。

例:

- 単一のデータベース インスタンスの場合：buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
- 複数のデータベースインスタンスの場合:
NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO|NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO
- **SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG** は、ストレージ システム名とボリューム名を含むスナップショットのリストを指定します。

例:

- 単一のデータベース インスタンスの場合
: buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- 複数のデータベースインスタンスの場合:
NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- **SC_PRIMARY_SNAPSHOT_NAMES** は、バックアップ中に作成されたプライマリスナップショットの名

前を指定します。

例:

- 単一データベースインスタンスの場合: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0、RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- 複数のデータベースインスタンスの場合: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0, RG2_scspr2417819002_07-21-2021_02.28.26.3973_1|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0, RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- 2つのボリュームを含む整合グループSnapshotの場合: cg3_R80404CBEF5V1_04-05-2021_03.08.03.4945_0_bfc279cc-28ad-465c-9d60-5487ac17b25d_2021_4_5_3_8_58_350

- **SC_PRIMARY_MOUNT_POINTS** は、バックアップの一部であるマウント ポイントの詳細を指定します。

詳細には、バックアップ対象のファイルの直接の親ではなく、ボリュームがマウントされているディレクトリが含まれます。ASM構成の場合は、ディスク グループの名前です。

データは <db1>@<mountpoint1,mountpoint2>|<db2>@<mountpoint1,mountpoint2> の形式になります。

例:

- 単一データベースインスタンスの場合: /mnt/nfsdb3_data、/mnt/nfsdb3_log、/mnt/nfsdb3_data1
- 複数のデータベースインスタンスの場合: NFSB31@/mnt/nfsdb31_data、/mnt/nfsdb31_log、/mnt/nfsdb31_data1|NFSB32@/mnt/nfsdb32_data、/mnt/nfsdb32_log、/mnt/nfsdb32_data1
- ASMの場合: +DATA2DG、+LOG2DG

- **SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS** は、各マウント ポイントのバックアップ中に作成されたスナップショットの名前を指定します。

例:

- 単一データベースインスタンスの場合: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data、RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log
- 複数のデータベースインスタンスの場合: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data, RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb31_data, RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb32_log

- **SC_ARCHIVELOGS_LOCATIONS** は、アーカイブ ログ ディレクトリの場所を指定します。

アーカイブ ログ ファイルの直接の親ディレクトリの名前になります。アーカイブ ログが複数の場所に配置されている場合は、すべての場所がキャプチャされます。これにはFRAのシナリオも含まれます。ディレクトリにソフトリンクが使用されている場合は、同じものが設定されます。

例:

- NFS上の単一データベースの場合: /mnt/nfsdb2_log
- NFS 上の複数のデータベースと、2 つの異なる場所に配置されている NFSB31 データベース アーカ

イブ ログの場合: NFSB31@/mnt/nfsdb31_log1、/mnt/nfsdb31_log2|NFSB32@/mnt/nfsdb32_log

◦ ASMの場合: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15

- **SC_REDO_LOGS_LOCATIONS** は、REDO ログ ディレクトリの場所を指定します。

Redoログ ファイルの直接の親ディレクトリの名前になります。ディレクトリにソフトリンクが使用されている場合は、同じものが設定されます。

例:

◦ NFS上の単一データベースの場合: /mnt/nfsdb2_data/newdb1

◦ NFS上の複数のデータベースの場合:
NFSB31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32

◦ ASMの場合: +LOG2DG/ASMDB2/ONLINELOG

- **SC_CONTROL_FILES_LOCATIONS** は制御ファイル ディレクトリの場所を指定します。

制御ファイルの直接の親ディレクトリの名前になります。ディレクトリにソフトリンクが使用されている場合は、同じものが設定されます。

例:

◦ NFS上の単一データベースの場合: /mnt/nfsdb2_data/fra/newdb1、/mnt/nfsdb2_data/newdb1

◦ NFS 上の複数のデータベースの場合:
NFSB31@/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/fra/newdb32,/mnt/nfsdb32_data/newdb32

◦ ASMの場合: +LOG2DG/ASMDB2/CONTROLFILE

- **SC_DATA_FILES_LOCATIONS** は、データ ファイル ディレクトリの場所を指定します。

データ ファイルの直接の親ディレクトリの名前になります。ディレクトリにソフトリンクが使用されている場合は、同じものが設定されます。

例:

◦ NFS上の単一データベースの場合: /mnt/nfsdb3_data1、/mnt/nfsdb3_data/NEWDB3/datafile

◦ NFS 上の複数のデータベースの場合:
NFSB31@/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/datafile|NFSB32@/mnt/nfsdb32_data1,/mnt/nfsdb32_data/NEWDB32/datafile

◦ ASMの場合: +DATA2DG/ASMDB2/DATAFILE、+DATA2DG/ASMDB2/TEMPFILE

- **SC_SNAPSHOT_LABEL** はセカンダリ ラベルの名前を指定します。

例: 時間別、日別、週別、月別、またはカスタム ラベル。

サポートされている区切り文字

- **:** は SVM 名とボリューム名を区切るために使用されます

例: buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_

07-21-2021_02.28.26.3973_1

- @ は、データとデータベース名を区別し、値とキーを区別するために使用されます。

例:

- NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- NFSB31@oracle|NFSB32@oracle
- | は、2 つの異なるデータベース間でデータを分離するため、および SC_BACKUP_ID、SC_BACKUP_RETENTION、および SC_BACKUP_NAME パラメータの 2 つの異なるエンティティ間でデータを分離するために使用されます。

例:

- DATA@203|LOG@205
- Hourly|DATA@DAYS:3|LOG@COUNT:4
- DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
- / は、SC_PRIMARY_SNAPSHOT_NAMES および SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG パラメータのボリューム名とそのスナップショットを区別するために使用されます。

例: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

- , は同じ DB の変数セットを区切るために使用されます。

例: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

バックアップ保持オプション

バックアップ コピーを保持する日数を選択するか、または保持するバックアップ コピーの数（ONTAPでは最大255個のコピー）を指定することができます。たとえば、組織の必要に応じて、10日分のバックアップ コピーや130個のバックアップ コピーを保持できます。

ポリシーを作成する際に、バックアップ タイプおよびスケジュール タイプの保持オプションを指定できます。

SnapMirrorレプリケーションを設定すると、デスティネーション ボリュームに保持ポリシーがミラーリングされます。

SnapCenter は、スケジュール タイプに一致する保持ラベルを持つ保持されたバックアップを削除します。リソースまたはリソース グループに対してスケジュール タイプが変更されると、古いスケジュール タイプラベルのバックアップがシステムに残ることがあります。



バックアップ コピーを長期にわたって保持する場合は、SnapVaultバックアップを使用する必要があります。

バックアップ スケジュール

バックアップ頻度（スケジュール タイプ）はポリシーで指定され、バックアップ スケジュールはリソース グループの設定で指定されます。バックアップの頻度またはスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率とデータの重要性です。使用頻度の高いリソースは1時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは1日に1回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービス レベル アグリーメント（SLA）、目標 復旧時点（RPO）などがあります。

SLAは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。RPOは、障害発生後に通常処理を再開するためにバックアップ ストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLAとRPOはデータ保護戦略に関わる要件です。

使用頻度の高いリソースであっても、フル バックアップは1日に1～2回で十分です。たとえば、定期的なトランザクション ログ バックアップを実行すれば、必要なバックアップが作成されます。データベースを頻繁にバックアップするほど、SnapCenterが復元時に使用するトランザクション ログが少なくなり、復元操作が高速化されます。

バックアップ スケジュールには、次の2つの要素があります。

- バックアップ頻度

バックアップ頻度 (バックアップを実行する頻度) は、一部のプラグインでは スケジュール タイプ と呼ばれ、ポリシー構成の一部です。ポリシーでは、バックアップ頻度として、毎時、毎日、毎週、または毎月を選択できます。頻度を選択しなかった場合は、オンデマンドのみのポリシーが作成されます。設定 > ポリシー をクリックすると、ポリシーにアクセスできます。

- バックアップ スケジュール

バックアップ スケジュール (バックアップが実行される日時) は、リソース グループ設定の一部です。たとえば、週次バックアップのポリシーが構成されたリソース グループがある場合は、毎週木曜日の午後 10 時にバックアップするようにスケジュールを構成できます。リソース > リソース グループ をクリックすると、リソース グループのスケジュールにアクセスできます。

バックアップの命名規則

Snapshotのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則ではSnapshot名にタイムスタンプが追加され

るので、コピーが作成されたタイミングを特定できます。

Snapshotでは、次のデフォルトの命名規則が使用されます。

```
resourcegroupname_hostname_timestamp
```

バックアップ リソース グループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- *dts1* はリソース グループ名です。
- *mach1x88* はホスト名です。
- *03-12-2015_23.17.26* は日付とタイムスタンプです。

または、[スナップショット コピーにカスタム名形式を使用する] を選択して、リソースまたはリソース グループを保護しながらスナップショット名の形式を指定することもできます。たとえば、`customtext_resourcegroup_policy_hostname`や`resourcegroup_hostname`などの形式です。デフォルトでは、Snapshot名にタイムスタンプのサフィックスが追加されます。

Oracleデータベースのバックアップの要件

Oracleデータベースをバックアップする前に、前提条件が満たされていることを確認する必要があります。

- ポリシーを適用したリソース グループを作成しておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。
- バックアップ処理で使用するアグリゲートを、データベースが使用するStorage Virtual Machine (SVM) に割り当てておく必要があります。
- データベースでセカンダリ保護が有効になっている場合は、そのデータベースに属しているすべてのデータ ボリュームとアーカイブ ログ ボリュームが保護されていることを確認する必要があります。
- Oracle DBVERIFY ユーティリティを使用してバックアップを検証するには、ASM ディスク グループ上にファイルを持つデータベースが「MOUNT」または「OPEN」のいずれかの状態であることを確認する必要があります。
- ボリューム マウント ポイントの長さが240文字を超えないことを確認しておく必要があります。
- バックアップ対象のデータベースが大きい場合 (サイズが TB 単位)、SnapCenter Server ホストの `C:\Program Files\NetApp\SMCore\SMCoreServiceHost.exe.config` ファイルで `RESTTimeout` の値を 86400000 ミリ秒に増やす必要があります。

値を変更する場合は実行中のジョブがないことを確認し、値を増やしたあとにSnapCenter SMCoreサービスを再起動してください。

バックアップに使用できるOracleデータベースの検出

リソースとなるのは、ホスト上でSnapCenterによって管理されているOracleデータベースです。使用できるデータベースを検出したあとに、それらのデータベースをリソースグループに追加してデータ保護処理を実行できます。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の作成、クレデンシャルの追加などのタスクを完了しておく必要があります。
- データベースが仮想マシン ディスク (VMDK) またはrawデバイス マッピング (RDM) にある場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。

詳細については、以下を参照してください。 ["SnapCenter Plug-in for VMware vSphereの導入"](#)。

- データベースが VMDK ファイル システム上に存在する場合は、vCenter にログインし、**VM オプション > 詳細 > 構成の編集** に移動して、VM の `disk.enableUUID` の値を `true` に設定する必要があります。
- さまざまなタイプとバージョンのOracleデータベースを検出するためにSnapCenterが実行するプロセスを確認しておく必要があります。

ステップ1: SnapCenterがデータベース以外のエントリを検出しないようにする

oratabファイルに追加されたデータベース以外のエントリがSnapCenterで検出されないようにすることができます。

手順

1. Oracle 用プラグインをインストールした後、root ユーザーはディレクトリ `/var/opt/snapcenter/sco/etc/` の下に **sc_oratab.config** ファイルを作成する必要があります。

Oracleバイナリの所有者とグループに書き込み権限を付与して、将来ファイルを管理できるようにします。

2. データベース管理者は、**sc_oratab.config** ファイルにデータベース以外のエントリを追加する必要があります。

`/etc/oratab` ファイル内の非データベース エントリに対して定義されているのと同じ形式を維持することをお勧めします。または、ユーザーは非データベース エンティティ文字列を追加するだけでもかまいません。



この文字列では大文字と小文字が区別されます。先頭に#が付いているテキストはコメントとして扱われます。コメントは非データベース名の後ろに追加できます。

```

For example:
-----
# Sample entries
# Each line can have only one non-database name
# These are non-database name
oratar # Added by the admin group -1
#Added by the script team
NEWSPT
DBAGNT:/ora01/app/oracle/product/agent:N
-----

```

3. リソースを検出します。

sc_oratab.config に追加されたデータベース以外のエントリは、リソース ページに表示されません。



SnapCenterプラグインをアップグレードする前に、sc_oratab.configファイルのバックアップを作成することを常に推奨します。

ステップ2: リソースの発見

プラグインをインストールすると、そのホスト上のすべてのデータベースが自動検出されて[Resources]ページに表示されます。

データベースが検出されるためには、データベースが少なくともマウント済み状態であることが必要です。Oracle Real Application Clusters (RAC) 環境で、検出が実行されるホスト内のRACデータベース インスタンスが検出されるためには、データベース インスタンスが少なくともマウント済み状態であることが必要です。正常に検出されたデータベースのみをリソース グループに追加できます。

ホスト上のOracleデータベースを削除した場合、SnapCenter Serverはそのことを認識せず、削除されたデータベースをリストに表示します。SnapCenterリソース リストを更新するには、リソースを手動で更新する必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] を選択します。

クリック  [フィルターアイコン] をクリックし、ホスト名とデータベースタイプを選択してリソースをフィルターします。次に、imagfilter_icon.gif[filter icon]_icon.png[] アイコンをクリックして、フィルター パネルを閉じることができます。

3. *リソースの更新*をクリックします。

RAC One Nodeシナリオでは、データベースが現在ホストされているノードでRACデータベースとして検出されます。

結果

データベースは、データベース タイプ、ホストまたはクラスタ名、関連するリソース グループとポリシー、

ステータスなどの情報とともに表示されます。



SnapCenterの外部でデータベースの名前が変更された場合は、リソースを更新する必要があります。

- データベースがNetApp以外のストレージ システムにある場合は、ユーザ インターフェイスの[Overall Status]列に「Not available for backup」というメッセージが表示されます。

NetApp以外のストレージにあるデータベースには、データ保護処理を実行できません。

- データベースがNetAppストレージ システムにあって保護されていない場合は、ユーザ インターフェイスの[Overall Status]列に「Not protected」というメッセージが表示されます。
- データベースがNetAppストレージ システムにあって保護されている場合は、ユーザ インターフェイスの[Overall Status]列に「Available for backup」というメッセージが表示されます。



Oracleデータベース認証が有効になっている場合は、リソース ビューに赤い南京錠アイコンが表示されます。データベースを保護できるようにデータベースのクレデンシャルを設定するか、またはデータベースをリソース グループに追加してデータ保護処理を実行する必要があります。

Oracleデータベースのバックアップ ポリシーの作成

SnapCenterを使用してOracleデータベース リソースをバックアップする前に、バックアップ対象のリソースまたはリソース グループのバックアップ ポリシーを作成する必要があります。バックアップ ポリシーとは、バックアップをどのように管理し、スケジューリングし、保持するかを定める一連のルールです。レプリケーション、スクリプト、バックアップ タイプの設定を指定することもできます。ポリシーを作成することで、別のリソースやリソース グループでポリシーを再利用したい場合に時間を節約できます。

始める前に

- バックアップ戦略を定義しておく必要があります。
- SnapCenterのインストール、ホストの追加、データベースの検出、ストレージ システム接続の作成などのタスクを実行して、データ保護の準備をしておく必要があります。
- Snapshotをミラー セカンダリ ストレージまたはバックアップ セカンダリ ストレージにレプリケートするユーザには、SnapCenter管理者がソースとデスティネーションの両方のボリューム用にSVMを割り当てる必要があります。
- root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプト ディレクトリとポストスクリプト ディレクトリに手動で割り当てる必要があります。
- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、["SnapMirrorアクティブ同期のオブジェクト数の制限"](#)。

タスク概要

[Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで指定した保持日数以下にする必要があります。

+ スナップショットのロック期間を指定すると、保持期間が終了するまでスナップショットが削除されなくな

ります。その結果、ポリシーで指定した数よりも多くのSnapshotが保持される可能性があります。

+ ONTAP 9.12.1 以下のバージョンでは、リストアの一環としてSnapLock Vault スナップショットから作成されたクローンには、SnapLock Vault の有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定] ページで、[ポリシー] をクリックします。
3. ドロップダウンリストから*Oracle Database*を選択します。
4. *新規* をクリックします。
5. 「名前」 ページで、ポリシー名と詳細を入力します。
6. ポリシー タイプ ページで、次の手順を実行します。

a. ストレージタイプを選択します。

b. ポリシーのスコープを選択:

- *オンライン バックアップを作成*する場合は、[オンライン バックアップ] を選択します。

データファイル、制御ファイル、アーカイブ ログ ファイルすべて、データファイルと制御ファイルのみ、アーカイブ ログ ファイルのみのいずれをバックアップするかを指定する必要があります。

- オフライン バックアップを作成*する場合は、[*オフライン バックアップ] を選択し、次のいずれかのオプションを選択します。

- データベースがマウントされた状態のときにオフライン バックアップを作成する場合は、[マウント] を選択します。

- データベースをシャットダウン状態に変更してオフライン シャットダウン バックアップを作成する場合は、「シャットダウン」を選択します。

プラグブル データベース (PDB) があり、バックアップを作成する前に PDB の状態を保存する場合は、「PDB の状態を保存」を選択する必要があります。これにより、バックアップ作成後にPDBを元の状態に戻すことができます。

- c. Oracle Recovery Manager (RMAN) を使用してバックアップをカタログ化する場合は、「**Oracle Recovery Manager (RMAN)** を使用したバックアップのカタログ化」を選択します。

GUIまたはSnapCenter CLIコマンドCatalog-SmBackupWithOracleRMANを使用して、一度に1つのバックアップのカタログ化を遅らせて実行できます。



RACデータベースのバックアップをカタログ化する場合は、そのデータベースに対して他のジョブが実行されていないことを確認します。別のジョブが実行されている場合は、カタログ化処理がキューに登録されずに失敗します。

- d. バックアップ後にアーカイブ ログを削除する場合は、[バックアップ後にアーカイブ ログを削除する] を選択します。



データベースで設定されていないアーカイブ ログ デスティネーションからのアーカイブ ログの削除はスキップされます。



Oracle Standard Editionを使用している場合は、アーカイブ ログのバックアップ中にLOG_ARCHIVE_DESTパラメータとLOG_ARCHIVE_DUPLEX_DESTパラメータを使用できます。

- アーカイブ ログを削除できるのは、アーカイブ ログ ファイルをバックアップの一部として選択した場合だけです。



削除処理を正常に行うためには、RAC環境のすべてのノードがすべてのアーカイブ ログの場所にアクセスできることを確認する必要があります。

状況	操作
すべてのアーカイブ ログを削除	*すべてのアーカイブ ログを削除*を選択します。
古いアーカイブ ログを削除	次の期間より古いアーカイブ ログを削除する を選択し、削除するアーカイブ ログの保存期間を日数と時間で指定します。
すべてのデスティネーションからアーカイブ ログを削除	すべての保存先からアーカイブ ログを削除する を選択します。
バックアップの一部であるログ デスティネーションからアーカイブ ログを削除	バックアップの一部である保存先からアーカイブ ログを削除する を選択します。

+

☒ Prune archive logs after backup

Prune log retention setting

☐ Delete all archive logs

☒ Delete archive logs older than

Prune log destination setting

☐ Delete archive logs from all the destinations

☒ Delete archive logs from the destinations which are part of backup

7. スナップショットとレプリケーション ページで、次の手順を実行します。

- オンデマンド、時間別、日次、週次、または*月次*を選択して、スケジュールの頻度を指定します。



リソース グループを作成する際に、バックアップ処理のスケジュール（開始日と終了日）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソース グループを作成できますが、各ポリシーに異なるバックアップ スケジュールを割り当てることもできます。



午前 2 時にスケジュールを設定した場合、夏時間 (DST) 中はスケジュールは実行されません。

- a. データ スナップショットの保持設定セクションで、バックアップ タイプ ページで選択したバックアップ タイプとスケジュール タイプの保持設定を指定します。

状況	操作
特定の数のSnapshotを保持	*保持するコピー*を選択し、保持するスナップショットの数を指定します。 Snapshotの数が指定した数を超えると、古いものから順にSnapshotが削除されます。 最大保持値は 1018 です。保持数を、使用しているONTAPバージョンがサポートする値よりも大きい値に設定すると、バックアップが失敗します。 SnapVaultレプリケーションを有効にする場合は、保持数を2以上に設定する必要があります。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。
Snapshotを特定の日数だけ保持	*コピーの保持期間*を選択し、スナップショットを削除する前に保持する日数を指定します。
スナップショットコピーのロック期間	スナップショット コピーのロック期間 を選択し、期間を日数、月数、または年数で指定します。 SnapLock保持期間は100年未満にする必要があります。

- b. アーカイブ ログ スナップショットの保持設定セクションで、バックアップ タイプ ページで選択したバックアップ タイプとスケジュール タイプの保持設定を指定します。

状況	操作

特定の数のSnapshotを保持	*保持するコピー*を選択し、保持するスナップショットの数を指定します。 Snapshotの数が指定した数を超えると、古いものから順にSnapshotが削除されます。  最大保持値は 1018 です。保持数を使用しているONTAPバージョンがサポートする値よりも大きい値に設定すると、バックアップが失敗します。  SnapVaultレプリケーションを有効にする場合は、保持数を2以上に設定する必要があります。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。
Snapshotを特定の日数だけ保持	*コピーの保持期間*を選択し、スナップショットを削除する前に保持する日数を指定します。
スナップショットコピーのロック期間	スナップショット コピーのロック期間 を選択し、期間を日数、月数、または年数で指定します。 SnapLock保持期間は100年未満にする必要があります。

c. ポリシーラベルを選択します。



リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしなくても実行できます。

8. [セカンダリ レプリケーション オプションの選択] セクションで、次のセカンダリ レプリケーション オプションの 1 つまたは両方を選択します。



セカンダリ スナップショット コピーのロック期間 を有効にするには、セカンダリ レプリケーション オプションを選択する必要があります。

フィールド	操作
Update SnapMirror after creating a local Snapshot	別のボリュームにバックアップ セットのミラー コピーを作成する場合（SnapMirrorレプリケーション）は、このフィールドを選択します。 このオプションは、SnapMirrorアクティブ同期に対して有効にする必要があります。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。 トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。
Update SnapVault after creating a local Snapshot	ディスクツーディスクのバックアップ レプリケーション（SnapVaultバックアップ）を実行する場合は、このオプションを選択します。 SnapLock がSnapLock Vault と呼ばれるONTAPのセカンダリにのみ設定されている場合、[トポロジ] ページの [更新] ボタンをクリックすると、ONTAPから取得されたセカンダリのロック期間が更新されます。 SnapLock Vaultの詳細については、"バックアップ デスティネーションのSnapshotコピーのWORM状態へのコミット" 見る"[Topology] ページでのOracleデータベースのバックアップとクローンの表示"。
Error retry count	処理が停止されるまでに試行できるレプリケーションの最大回数を入力します。



セカンダリ ストレージでSnapshotの上限に達しないように、ONTAPでセカンダリ ストレージのSnapMirror保持ポリシーを設定する必要があります。

9. [Script]ページで、バックアップ処理の前またはあとに実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

プレスクリプトとポストスクリプトは、`/var/opt/snapcenter/spl/scripts` またはこのパス内の任意のフォルダーに保存する必要があります。デフォルトでは、`/var/opt/snapcenter/spl/scripts` パスが設定されます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

スクリプトのタイムアウト値を指定することもできます。デフォルト値は60秒です。

SnapCenter、事前スクリプトと事後スクリプトを実行するときに、事前定義された環境変数を使用できま

す。"詳細情報"

10. [Verification]ページで、次の手順を実行します。

- a. 検証処理の実行対象となるバックアップ スケジュールを選択します。
- b. [Verification script commands]セクションで、検証処理の前後に実行するプリスクリプトまたはポストスクリプトの引数とパスを入力します。

プレスクリプトとポストスクリプトは、`/var/opt/snapcenter/spl/scripts` またはこのパス内の任意のフォルダーに保存する必要があります。デフォルトでは、`/var/opt/snapcenter/spl/scripts` パスが設定されます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

スクリプトのタイムアウト値を指定することもできます。デフォルト値は60秒です。

11. 概要を確認し、[完了] をクリックします。

Oracleデータベースのリソース グループの作成とポリシーの適用

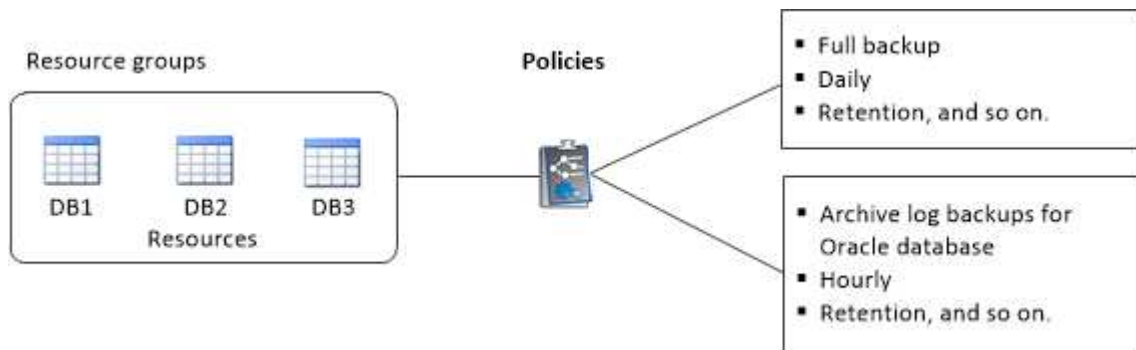
リソース グループはコンテナであり、バックアップして保護するリソースをここに追加します。リソース グループを使用することで、特定のアプリケーションに関連するすべてのデータを同時にバックアップできます。

タスク概要

- Oracle DBVERIFYユーティリティを使用してバックアップを検証するには、ASMディスク グループにファイルが格納されているデータベースが「MOUNT」または「OPEN」状態である必要があります。

リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義します。

次の図は、データベースのリソース、リソース グループ、ポリシーの関係を示しています。



- SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotのロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期を使用するリソースを含む既存のリソース グループにSnapMirrorアクティブ同期を使用しない新しいデータベースを追加することはできません。
- SnapMirrorアクティブ同期のフェイルオーバー モードである既存のリソース グループに新しいデータベースを追加することはできません。リソースを追加できるのは、通常の状態またはフェイルバック状態のリソース グループのみです。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。
 - a. [Name] フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag] フィールドに1つ以上のラベルを入力します。

たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

- c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- d. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。



必要に応じて、プレフィックスも含めて、Oracleで設定されたものとまったく同じデスティネーションを使用してください。

4. [リソース] ページで、[ホスト] ドロップダウン リストから Oracle データベース ホスト名を選択します。



[Available Resources] セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources] のリストには表示されません。

5. [Available Resources] セクションでリソースを選択し、[Selected Resources] セクションに移動します。



1つのリソース グループ内のLinuxホストとAIXホストの両方からデータベースを追加できます。

6. アプリケーション設定ページで、バックアップ オプションを選択します。

7. [Policies] ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックし  てポリシーを作成することもできます。

[Configure schedules for selected policies] セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。

- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. [Verification]ページで、次の手順を実行します。

- a. ロケーターのロード をクリックして、 SnapMirrorまたはSnapVaultボリュームをロードし、セカンダリストレージで検証を実行します。
- b. クリック  ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で をクリックします。
- c. [Add Verification Schedules *policy_name*]ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

- d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証]を選択します。
- e. [OK]をクリックします。

設定した検証スケジュールが、[Applied Schedules]列にリストされます。

9. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtplibServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

10. 概要を確認し、[完了] をクリックします。

リソース グループを作成し、 **ASA r2** システム上の **Oracle** リソースの二次保護を有効にします。

ASA r2 システム上にあるリソースを追加するには、リソース グループを作成する必要があります。リソース グループの作成時にセカンダリ保護をプロビジョニングすること

もできます。

開始する前に

- ONTAP 9.x リソースとASA r2 リソースの両方を同じリソース グループに追加していないことを確認する必要があります。
- ONTAP 9.x リソースとASA r2 リソースの両方を含むデータベースが存在しないことを確認する必要があります。

タスク概要

- 二次保護は、ログインしたユーザーに **SecondaryProtection** 機能が有効になっているロールが割り当てられている場合にのみ使用できます。
- セカンダリ保護を有効にすると、プライマリおよびセカンダリ整合性グループの作成中にリソース グループはメンテナンス モードになります。プライマリおよびセカンダリのコンシステンシー グループが作成されると、リソース グループのメンテナンス モードが解除されます。
- SnapCenter はクローン リソースの二次保護をサポートしていません。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。
 - a. [Name] フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag] フィールドに1つ以上のラベルを入力します。

たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

- c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- d. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。



必要に応じて、プレフィックスを含め、アプリケーションで設定されたのと同まったく同じ宛先を使用する必要があります。

4. [リソース] ページで、[ホスト] ドロップダウン リストからデータベース ホスト名を選択します。



[Available Resources] セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources] のリストには表示されません。

5. [使用可能なリソース] セクションからASA r2 リソースを選択し、[選択したリソース] セクションに移動し

ます。

6. アプリケーション設定ページで、バックアップ オプションを選択します。
7. [Policies]ページで、次の手順を実行します。
 - a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックし  てポリシーを作成することもできます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、  をクリックします。
- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 選択したポリシーに対して二次保護が有効になっている場合は、「二次保護」ページが表示されるので、次の手順を実行する必要があります。
 - a. レプリケーション ポリシーのタイプを選択します。



同期レプリケーション ポリシーはサポートされていません。

- b. 使用する整合性グループのサフィックスを指定します。
- c. [宛先クラスタ] および [宛先 SVM] ドロップダウンから、使用するピア クラスタと SVM を選択します。



クラスタと SVM のピアリングはSnapCenterではサポートされていません。クラスタと SVM のピアリングを実行するには、System Manager またはONTAP CLI を使用する必要があります。



リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは [セカンダリ保護リソース] セクションに表示されます。

1. [Verification]ページで、次の手順を実行します。
 - a. ロケータのロード をクリックして、 SnapMirrorまたはSnapVaultボリュームをロードし、セカンダリストレージで検証を実行します。
 - b. クリック  ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で をクリックします。
 - c. [Add Verification Schedules *policy_name*]ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

- d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証] を選択します。
- e. [OK]をクリックします。

設定した検証スケジュールが、[Applied Schedules]列にリストされます。

2. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

3. 概要を確認し、[完了] をクリックします。

Oracleリソースのバックアップ

どのリソース グループにもまだ含まれていないリソースは、[Resources]ページからバックアップすることができます。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから データベース を選択します。
3. をクリックし、ホスト名とデータベース タイプを選択してリソースをフィルタします。

そのあとにをクリックすると、フィルタ ペインが閉じます。

4. バックアップするデータベースを選択します。

[Database-Protect]ページが表示されます。

5. [Resources]ページで、次の手順を実行します。
 - a. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

例えば、 customtext_policy_hostname`または `resource_hostname。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

b. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。

6. [Policies]ページで、次の手順を実行します。

a. ドロップダウン リストから1つ以上のポリシーを選択します。

クリックするとポリシーを作成できます 。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

b. クリック  必要なポリシーのスケジュールを構成するには、[スケジュールの構成] 列をクリックします。

c. 「ポリシー_policy_name_のスケジュールを追加」ウィンドウでスケジュールを設定し、OK。

policy_name は、選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

7. [Verification]ページで、次の手順を実行します。

a. ロケーターのロード をクリックして、SnapMirrorまたはSnapVaultボリュームをロードし、セカンダリストレージを検証します。

b. クリック  ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で をクリックします。 + 「検証スケジュールの追加 *policy_name*」ダイアログ ボックスで、次の手順を実行できます。

c. *バックアップ後に検証を実行*を選択します。

d. *スケジュールされた検証を実行する*を選択し、ドロップダウン リストからスケジュールの種類を選択します。



Flex ASMセットアップでは、カーディナリティがRACクラスタ内のノード数より少ない場合、リーフ ノードで検証処理を実行できません。

e. セカンダリ ストレージ上のバックアップを検証するには、[セカンダリ ロケーションで検証] を選択します。

f. [OK]をクリックします。

設定した検証スケジュールが、[Applied Schedules]列にリストされます。

8. 通知ページで、*電子メール設定*ドロップダウンリストから電子メールを送信するシナリオを選択します。

送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースに対して実行されたバックアップ操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



電子メール通知の場合は、GUIまたはPowerShellコマンドを使用してSMTPサーバーの詳細を指定する必要があります。 `Set-SmSmtServer`。

9. 概要を確認し、[完了] をクリックします。

データベース トポロジのページが表示されます。

10. *今すぐバックアップ*をクリックします。

11. [Backup]ページで次の手順を実行します。

- a. リソースに複数のポリシーを適用した場合は、バックアップに使用するポリシーを[Policy]ドロップダウン リストから選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*をクリックします。

12. モニター > ジョブ をクリックして、操作の進行状況を監視します。

終了後の操作

- AIXセットアップでは、`lkdev`ロックするコマンドと`rendev`バックアップされたデータベースが保存されていたディスクの名前を変更するコマンド。

そのバックアップを使用してリストアを実行する際、デバイスのロックおよび名前変更がリストア処理に影響することはありません。

- データベースクエリの実行時間がタイムアウト値を超えたためにバックアップ操作が失敗した場合は、以下のコマンドを実行してORACLE_SQL_QUERY_TIMEOUTおよびORACLE_PLUGIN_SQL_QUERY_TIMEOUTパラメータの値を変更する必要があります。`Set-SmConfigSettings` コマンドレット:

パラメータの値を変更した後、次のコマンドを実行してSnapCenter Plug-in Loader (SPL)サービスを再起動します。 `/opt/NetApp/snapcenter/spl/bin/spl restart`

- ファイルにアクセスできず、検証プロセス中にマウント ポイントを使用できない場合、処理が失敗し、エラー コードDBV-00100 Specified FILEが表示されることがあります。sco.propertiesのVERIFICATION_DELAYおよびVERIFICATION_RETRY_COUNTパラメータの値を変更する必要があります。

パラメータの値を変更した後、次のコマンドを実行してSnapCenter Plug-in Loader (SPL)サービスを再起動します。 `/opt/NetApp/snapcenter/spl/bin/spl restart`

- MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。
- VMDK上のアプリケーション データをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープ サイズが不足していると、バックアップが失敗することがあります。

Java ヒープ サイズを増やすには、スクリプト ファイル `/opt/netapp/init_scripts/scvservice` を見つけます。その脚本では、`do_start method`` コマンドは、SnapCenter VMware プラグイン サービスを開始します。このコマンドを次のように更新します。 ``Java -jar -Xmx8192M -Xms4096M。`

詳細情報の参照

- ["MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"](#)
- ["Oracle RAC One NodeデータベースはSnapCenter操作の実行ではスキップされます"](#)
- ["Oracle 12c ASMデータベースの状態を変更できませんでした"](#)

- "AIX システムでのバックアップ、復元、クローン操作のカスタマイズ可能なパラメータ" (ログインが必要です)

Oracle データベースのリソース グループのバックアップ

リソース グループは、ホストまたはクラスタ上のリソースの集まりです。バックアップ処理は、リソース グループに定義されているすべてのリソースに対して実行されます。

リソース グループは、[Resources] ページからオンデマンドでバックアップできます。リソース グループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従ってバックアップが作成されます。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。
3. 検索ボックスにリソースグループ名を入力するか、 をクリックして、タグを選択します。

 をクリックし  でフィルタ ペインを閉じます。

4. [Resource Group] ページで、バックアップするリソース グループを選択します。



2つのデータベースが統合されたリソース グループがある場合に、一方のデータベースのデータがNetApp以外のストレージにあると、もう一方のデータベースがNetAppストレージにあっても、バックアップ処理は中止されます。

5. [Backup] ページで次の手順を実行します。
 - a. リソース グループに複数のポリシーが関連付けられている場合は、[ポリシー] ドロップダウン リストから使用するバックアップ ポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*を選択します。
6. モニター > ジョブ を選択して進行状況を監視します。

終了後の操作

- AIX セットアップでは、`lkdev` ロックするコマンドと `rendev` バックアップされたデータベースが保存されていたディスクの名前を変更するコマンド。

そのバックアップを使用してリストアを実行する際、デバイスのロックおよび名前変更がリストア処理に影響することはありません。

- データベースクエリの実行時間がタイムアウト値を超えたためにバックアップ操作が失敗した場合は、以下のコマンドを実行してORACLE_SQL_QUERY_TIMEOUTおよびORACLE_PLUGIN_SQL_QUERY_TIMEOUTパラメータの値を変更する必要があります。`Set-SmConfigSettings` コマンドレット:

パラメータの値を変更した後、次のコマンドを実行してSnapCenter Plug-in Loader (SPL) サービスを再起動します。`/opt/NetApp/snapcenter/spl/bin/spl restart`

- ファイルにアクセスできず、検証プロセス中にマウント ポイントを使用できない場合、処理が失敗し、エラー コード DBV-00100 Specified FILEが表示されることがあります。sco.properties の VERIFICATION_DELAY_ および VERIFICATION_RETRY_COUNT パラメータの値を変更する必要があります。

パラメータの値を変更した後、次のコマンドを実行してSnapCenter Plug-in Loader (SPL)サービスを再起動します。 /opt/NetApp/snapcenter/spl/bin/spl restart

Oracleデータベースのバックアップの監視

バックアップ処理とデータ保護処理の進捗状況を監視する方法について説明します。

Oracleデータベースのバックアップ処理の監視

SnapCenterの[Jobs]ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*ジョブ*をクリックします。
3. [Jobs]ページで、次の手順を実行します。
 - a. をクリックして、 リストの内容をバックアップ処理だけに絞り込みます。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*バックアップ*を選択します。
 - d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. バックアップ ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスは  ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[Activity]ペインでデータ保護処理を監視

[Activity]ペインには、最後に実行された5つの処理が表示されます。また[Activity]ペインには、処理が開始された日次と処理のステータスが表示されます。

[Activity]ペインには、バックアップ、リストア、クローニング、スケジュールされたバックアップの各処理に関する情報が表示されます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. クリック  アクティビティ ペインで、最新の 5 つの操作を表示します。

いずれかの操作をクリックすると、*ジョブの詳細*ページに操作の詳細が表示されます。

その他のバックアップ処理

UNIXコマンドを使用したOracleデータベースのバックアップ

バックアップのワークフローには、計画、バックアップするリソースの特定、バックアップ ポリシーの作成、リソース グループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

必要なもの

- *Add-SmStorageConnection* コマンドと *Add-SmCredential* コマンドを使用して、ストレージ システム接続を追加し、資格情報を作成しておく必要があります。
- *Open-SmConnection* コマンドを使用して、 SnapCenter Server との接続セッションを確立しておく必要があります。

SnapCenterアカウントでのログイン セッションは1つしか確立できず、トークンはユーザのホーム ディレクトリに保存されます。



接続セッションは24時間を過ぎると無効になります。ただし、TokenNeverExpiresオプションを使用して期限切れにならないトークンを作成し、セッションが無効にならないようにすることができます。

このタスクについて

次に示すコマンドを実行して、SnapCenter Serverとの接続の確立、Oracleデータベース インスタンスの検出、ポリシーとリソース グループの追加、バックアップの作成と検証を行います。

コマンドで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンド リファレンス ガイド](#)"。

手順

1. 指定されたユーザーのSnapCenter Server との接続セッションを開始します: *Open-SmConnection*
2. ホスト リソース検出操作を実行します: *Get-SmResources*
3. Real Application Cluster (RAC) データベースのバックアップ操作用に Oracle データベースの資格情報と優先ノードを構成します: *Configure-SmOracleDatabase*
4. バックアップポリシーを作成します: *Add-SmPolicy*
5. セカンダリ (SnapVaultまたはSnapMirror) ストレージの場所に関する情報を取得します: *Get-SmSecondaryDetails*

このコマンドでは、指定したリソースのプライマリ ストレージからセカンダリ ストレージへのマッピングの詳細が取得されます。バックアップ リソース グループを作成する際に、このマッピングの詳細を使用してセカンダリの検証を設定できます。

6. SnapCenterにリソース グループを追加します: *Add-SmResourceGroup*
7. バックアップを作成します: *New-SmBackup*

WaitForCompletionオプションを使用してジョブをポーリングすることができます。このオプションを指定しない場合は、バックアップ ジョブが完了するまでコマンドが引き続きサーバをポーリングします。

8. SnapCenterからログを取得します: *Get-SmLogs*

Oracleデータベースのバックアップ処理のキャンセル

実行中のバックアップ処理、キューに登録されたバックアップ処理、応答しないバックアップ処理をキャンセルできます。

バックアップ処理をキャンセルするには、SnapCenter管理者またはジョブ所有者としてログインする必要があります。

このタスクについて

バックアップ処理をキャンセルすると、SnapCenter Serverにより処理が停止されます。作成されたバックアップがSnapCenter Serverに登録されていない場合、ストレージからすべてのSnapshotが削除されます。バックアップがすでにSnapCenter Serverに登録されている場合、キャンセルがトリガーされても、すでに作成されているSnapshotはロールバックされません。

- キャンセルできるのは、キューに登録されているか実行中のログ バックアップまたはフル バックアップの処理だけです。
- 検証の開始後は、処理をキャンセルできません。

検証前に処理をキャンセルすると、処理はキャンセルされ、検証処理は実行されません。

- カタログ処理が開始されたあとにバックアップ処理をキャンセルすることはできません。
- バックアップ処理は、[Monitor]ページまたは[Activity]ペインでキャンセルできます。
- SnapCenter GUIからだけでなく、CLIコマンドを使用して処理をキャンセルすることもできます。
- キャンセルできない操作の場合、「ジョブのキャンセル」ボタンは無効になります。

- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたバックアップ操作をキャンセルできます。

ステップ

次のいずれかを実行します。

方法	アクション
[Monitor]ページ	1. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 2. 操作を選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	1. バックアップジョブを開始したら、 アクティビティ ペインで、最新の 5 つの操作を表示します。 2. 処理を選択します。 3. ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

結果

処理がキャンセルされ、リソースが元の状態に戻ります。

キャンセルした操作がキャンセル中または実行中の状態で応答しない場合は、Cancel-SmJob -JobID <int> -Force を実行して、バックアップ操作を強制的に停止する必要があります。

[Topology]ページでのOracleデータベースのバックアップとクローンの表示

リソースのバックアップまたはクローニングを準備する際に、プライマリ ストレージとセカンダリ ストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。

このタスクについて

[Topology]ページでは、選択したリソースまたはリソース グループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を参照し、対象を選択してデータ保護処理を実行できます。

プライマリ ストレージまたはセカンダリ ストレージ（ミラー コピーまたはバックアップ コピー）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

-  プライマリ ストレージで使用可能なバックアップとクローンの数を表示します。
-



SnapMirrorテクノロジーを使用してセカンダリ ストレージにミラーリングされているバックアップとクローンの数を表示します。



SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップとクローンの数を表示します。

表示されるバックアップの数には、セカンダリ ストレージから削除されたバックアップも含まれます。たとえば、バックアップを4個保持するポリシーを使用してバックアップを6個作成した場合、バックアップの数は6個と表示されます。



mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジ ビューに表示されますが、トポロジ ビューのミラー バックアップの数にはバージョンに依存しないバックアップは含まれません。

SnapMirrorアクティブ同期 (当初はSnapMirror Business Continuity [SM-BC] としてリリース) としてセカンダリ関係がある場合は、次の追加アイコンが表示されます。



レプリカサイトが稼働しています。



レプリカサイトはダウンしています。



セカンダリ ミラーまたはボルト関係が再確立されていません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストからリソースまたはリソース グループを選択します。
3. リソースの詳細ビューまたはリソース グループの詳細ビューで、リソースを選択します。

リソースが保護されている場合は、選択したリソースの[Topology]ページが表示されます。

4. [Summary Card]で、プライマリ ストレージとセカンダリ ストレージ上にあるバックアップとクローンの数の概要を確認します。

[Summary Card]セクションには、バックアップとクローンの総数およびログ バックアップの総数が表示されます。

更新 ボタンをクリックすると、ストレージのクエリが開始され、正確な数が表示されます。

SnapLock対応バックアップが取得された場合、[更新] ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでも、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

アプリケーション リソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限はONTAPから取得されます。

SnapMirrorアクティブ同期の場合、[更新] ボタンをクリックすると、プライマリ サイトとレプリカ サイトの両方に対してONTAP を照会してSnapCenterバックアップ インベントリが更新されます。週次スケジュールでも、SnapMirrorアクティブ同期関係を含むすべてのデータベースに対してこの処理が実行されます。

- SnapMirrorアクティブ同期とONTAP（バージョン9.14.1のみ）では、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップの関係については、フェイルオーバー後に手動で設定する必要があります。ONTAP 9.15.1以降は、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップが、自動的に設定されます。
 - フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。バックアップが作成された後にのみ、「更新」をクリックできます。
5. 「コピーの管理」ビューで、プライマリ ストレージまたはセカンダリ ストレージから バックアップ または クローン をクリックして、バックアップまたはクローンの詳細を表示します。

バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、マウント、アンマウント、名前変更、カタログ化、カタログ解除、削除の各処理を実行します。



セカンダリ ストレージ上のバックアップは、名前変更または削除できません。

- ログ バックアップを選択した場合は、名前の変更、マウント、マウント解除、カタログ、カタログ解除、および削除の操作のみを実行できます。
 - Oracle Recovery Manager（RMAN）を使用してバックアップをカタログ化した場合、そのバックアップの名前は変更できません。
7. クローンを削除する場合は、表でクローンを選択し、 をクリックします。

SnapmirrorStatusUpdateWaitTimeに割り当てられている値が小さい場合は、データ ボリュームとログ ボリュームが正常に保護されていても、ミラーとバックアップのバックアップ コピーはトポロジ ページに表示されません。Set-SmConfigSettings PowerShell コマンドレットを使用して、SnapmirrorStatusUpdateWaitTime に割り当てられた値を増やす必要があります。

コマンドで利用できるパラメータとその説明に関する情報は、Get-Help *command_name* を実行すると取得できます。

あるいは、["SnapCenterソフトウェア コマンド リファレンス ガイド"](#)または["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

データベース バックアップのマウントとアンマウント

バックアップ内のファイルにアクセスする必要がある場合は、1つまたは複数のデータ バックアップや、ログのみのバックアップをマウントできます。バックアップは、バックアップが作成されたホストにも、同じタイプのOracleおよびホスト構成を使用するリモート ホストにもマウントできます。バックアップを手動でマウントした場合は、処理の完了後にバックアップを手動でアンマウントする必要があります。任意のインスタンスで、データベースのバックアップを任意のホストにマウントできます。処理を実行する際には、バックアップを1つだけマウントできます。



Flex ASMセットアップでは、カーディナリティがRACクラスタ内のノード数より少ない場合、リーフ ノードでマウント処理を実行できません。

データベース バックアップをマウントする

バックアップ内のファイルにアクセスする必要がある場合は、データベース バックアップを手動でマウントします。

必要なもの

- NFS 環境に Automatic Storage Management (ASM) データベース インスタンスがあり、ASM バックアップをマウントする場合は、asm_diskstring パラメータで定義されている既存のパスに ASM ディスク パス `/var/opt/snapcenter/sco/backup*/**/*` を追加する必要があります。
- NFS 環境に ASM データベース インスタンスがあり、リカバリ操作の一環として ASM ログ バックアップをマウントする場合は、asm_diskstring パラメータで定義されている既存のパスに ASM ディスク パス `/var/opt/snapcenter/scu/clones/*/*` を追加する必要があります。
- asm_diskstring パラメータでは、ASMFD を使用している場合は `AFD:*` を構成し、ASMLIB を使用している場合は `ORCL:*` を構成する必要があります。



asm_diskstringパラメータを編集する方法については、以下を参照してください。
["asm_diskstringにディスクパスを追加する方法"](#)。

- バックアップのマウント時に使うASMクレデンシャルとASMポートがソース データベース ホストのものと異なる場合は、ASMクレデンシャルとASMポートを設定する必要があります。
- 代替ホストにマウントする場合は、代替ホストが次の要件を満たしていることを確認する必要があります。
 - UIDとGIDが元のホストと同じである
 - 元のホストと同じOracleバージョン
 - 元のホストと同じOSディストリビューションとバージョン
 - NVMeの場合は、NVMeユーティリティがインストールされている必要があります。
- iSCSIプロトコルとFCプロトコルが混在するigroupを使用して、LUNがAIXホストにマッピングされていないことを確認します。詳細については、以下を参照してください。 ["LUNのデバイスを検出できないというエラーが発生し、操作が失敗しました"](#)。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] または [リソース グループ] を選択します。
3. データベースの詳細ビューまたはリソース グループの詳細ビューでデータベースを選択します。

データベース トポロジのページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたは複製) ストレージ システムから [バックアップ] を選択します。
5. 表からバックアップを選択し、クリックします 。

6. [バックアップのマウント] ページで、[バックアップをマウントするホストを選択] ドロップダウン リストから、バックアップをマウントするホストを選択します。

マウント パス `/var/opt/snapcenter/sco/backup_mount/backup_name/database_name` が表示されます。

ASM データベースのバックアップをマウントしている場合は、マウント パス `+diskgroupname_SID_backupid` が表示されます。

7. *マウント*をクリックします。

終わったら

- 次のコマンドを実行して、マウントされたバックアップに関する情報を取得できます。

```
./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
```

- ASMデータベースをマウントした場合に、マウントされたバックアップに関する情報を取得するには、次のコマンドを実行します。

```
./sccli Get-Smbbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
```

- バックアップIDを取得するには、次のコマンドを実行します。

```
./sccli Get-Smbbackup-BackupNamebackup_name
```

コマンドで使用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンド リファレンス ガイド](#)"。

データベース バックアップをアンマウントする

マウントされたデータベース バックアップ上のファイルにアクセスする必要がなくなった場合は、そのバックアップを手動でアンマウントできます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] または [リソース グループ] を選択します。
3. データベースの詳細ビューまたはリソース グループの詳細ビューでデータベースを選択します。

データベース トポロジのページが表示されます。

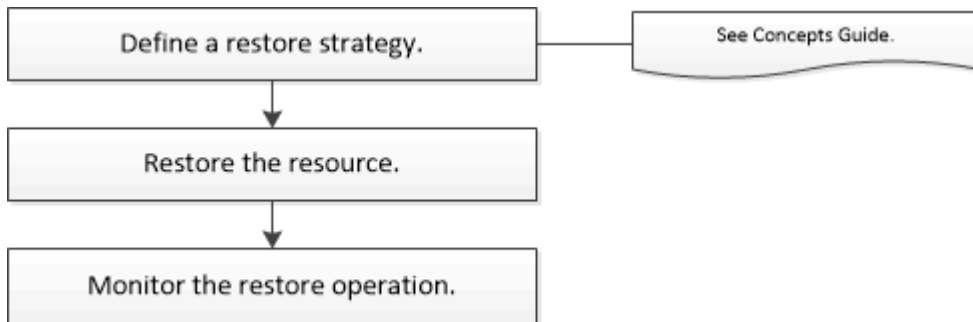
4. マウントされているバックアップを選択し、クリックします 。
5. [OK]をクリックします。

Oracleデータベースのリストアとリカバリ

リストアのワークフロー

リストア ワークフローには、計画、リストア処理の実行、および処理の監視が含まれます。

次のワークフローは、リストア処理の実行順序を示しています。



Oracle データベースのリストアおよびリカバリ戦略の定義

データベースのリストアとリカバリを行う前に戦略を定義しておく、リストア処理とリカバリ処理を正常に実行できるようになります。

リストア処理とリカバリ処理でサポートされるバックアップのタイプ

SnapCenterでは、さまざまなタイプのOracle データベース バックアップのリストアとリカバリがサポートされます。

- オンライン データ バックアップ
- オフライン シャットダウン データ バックアップ
- オフライン マウント データ バックアップ



オフライン シャットダウンまたはオフライン マウント データ バックアップをリストアする場合、SnapCenterはデータベースをオフライン状態のままにします。データベースを手動でリカバリし、ログをリセットする必要があります。

- フル バックアップ
- Data Guardスタンバイ データベースのオフライン マウント バックアップ
- Active Data Guardスタンバイ データベースのデータのみのオンライン バックアップ



Active Data Guardスタンバイ データベースのリカバリは実行できません。

- Real Application Clusters (RAC) 構成でのオンライン データ バックアップ、オンライン フル バックアップ、オフライン マウント バックアップ、オフライン シャットダウン バックアップ
- Automatic Storage Management (ASM) 構成でのオンライン データ バックアップ、オンライン フル バックアップ、オフライン マウント バックアップ、オフライン シャットダウン バックアップ

Oracleデータベースでサポートされるリストア方式のタイプ

SnapCenterでは、Oracleデータベースに対してConnect and CopyリストアとIn Placeリストアがサポートされます。SnapCenterは、リストア処理時に、リストアに使用されるファイルシステムでデータ損失が生じないようにするための適切なリストア方式を決定します。



SnapCenterでは、ボリュームベースのSnapRestoreはサポートされません。

Connect and Copyリストア

データベース レイアウトがバックアップと異なる場合や、バックアップ作成後にファイルが追加された場合は、Connect and Copyリストアが実行されます。Connect and Copyリストア方式では、次のタスクが実行されます。

手順

1. Snapshotからボリュームがクローニングされ、クローニングされたLUNまたはボリュームを使用してホスト上にファイルシステム スタックが構築されます。
2. クローニングされたファイルシステムから元のファイルシステムにファイルがコピーされます。
3. クローニングされたファイルシステムがホストからアンマウントされ、クローニングされたボリュームがONTAPから削除されます。



Flex ASMセットアップ（RACクラスタ内のノード数よりもカーディナリティが少ない）またはVMDKかRDM上のASM RACデータベースでは、Connect and Copyリストア方式のみがサポートされます。

In Placeリストアを強制的に有効にした場合でも、次のシナリオではSnapCenterがConnect and Copyリストアを実行します。

- セカンダリストレージシステムからの復元
- データベース インスタンスが設定されていないOracle RACセットアップのノードに存在するASMディスク グループをリストアする場合
- Oracle RACセットアップで、いずれかのピア ノードでASMインスタンスまたはクラスタ インスタンスが実行されていない場合、またはピア ノード自体が停止している場合
- 制御ファイルのみをリストアする場合
- ASMディスク グループに存在する表領域の一部をリストアする場合
- ディスク グループがデータ ファイル、spファイル、パスワード ファイルの間に共有されている場合
- RAC環境のリモート ノードで、SnapCenter Plug-in Loader（SPL）サービスがインストールされていないか実行されていない場合
- Oracle RACに新たに追加されたノードがSnapCenter Serverで認識されていない場合

In Placeリストア

データベース レイアウトがバックアップとほぼ同じであり、かつストレージとデータベース スタックで設定変更が行われていない場合は、In Placeリストアが実行されて、ファイルまたはLUNのリストアがONTAP上で実行されます。SnapCenterでは、In Placeリストア方式の一環としてSingle File SnapRestore（SFSR）のみがサポートされます。



NetApp ONTAP は、セカンダリ ロケーションからのインプレース リストアをサポートします。

データベースでIn Placeリストアを実行する場合は、ASMディスク グループにデータファイルだけがあることを確認してください。ASMディスク グループまたはデータベースの物理構造に変更を加えた場合は、バックアップを作成する必要があります。In Placeリストアを実行すると、ディスク グループにバックアップ時と同じ数のデータファイルが格納されます。

ディスク グループまたはマウント ポイントが次の基準と一致する場合は、In Placeリストアが自動的に適用されます。

- バックアップ後に新しいデータファイルが追加されていない（外部ファイル チェック）
- バックアップ後にASMディスク またはLUNの追加、削除、または再作成が行われていない（ASMディスク グループの構造変更チェック）
- LVMディスク グループに対してLUNの追加、削除、または再作成が行われていない（LVMディスク グループの構造変更チェック）



In Placeリストアを強制的に有効にすることもできます。有効にするには、GUI、SnapCenter CLI、またはPowerShellコマンドレットを使用して、外部ファイル チェックおよびLVMディスク グループの構造変更チェックを無効にします。

ASM RACでのIn Placeリストアの実行

SnapCenterでは、リストアを実行するノードがプライマリ ノードと呼ばれ、ASMディスク グループがあるRAC上のその他すべてのノードがピア ノードと呼ばれます。SnapCenterは、ストレージ リストア処理を実行する前に、ASMディスク グループがマウント状態にあるすべてのノードで、ディスクマウントするASMディスク グループの状態を変更します。ストレージのリストアが完了すると、SnapCenterはASMディスク グループの状態をリストア処理前の状態に変更します。

SAN環境では、ストレージ リストア処理の前に、SnapCenterがすべてのピア ノードからデバイスを削除し、LUNのマッピング解除処理を実行します。ストレージ リストア処理が完了すると、SnapCenterはLUNマッピング処理を実行し、すべてのピア ノードでデバイスを構築します。SAN環境のLUN上にOracle RAC ASMレイアウトが存在する場合は、リストア中に、ASMディスク グループが存在するRACクラスタのすべてのノードでSnapCenterがLUNのマッピング解除、LUNのリストア、およびLUNのマッピングを実行します。リストア前にRACノードのすべてのイニシエータがLUNに使用されていなかった場合でも、リストア後はSnapCenterがすべてのRACノードのすべてのイニシエータを含む新しいigroupを作成します。

- ピア ノードでリストア前の処理中にエラーが発生した場合は、リストア前の処理が成功したピア ノードでSnapCenterが自動的にASMディスク グループの状態をリストア実行前の状態にロールバックします。プライマリ ノードおよび処理が失敗したピア ノードでは、ロールバックがサポートされません。新たなリストアを実行する前に、ピア ノードの問題を手動で修正し、プライマリ ノード上のASMディスク グループをマウント状態に戻す必要があります。
- リストア処理中にエラーが発生した場合は、リストア処理が失敗し、ロールバックは実行されません。新たなリストアを実行する前に、ストレージ リストアの問題を手動で修正し、プライマリ ノード上のASMディスク グループをマウント状態に戻す必要があります。
- いずれかのピア ノードでリストア後の処理中にエラーが発生した場合、SnapCenterは他のピア ノードでリストア処理を続行します。このピア ノードでリストア後の問題を手動で修正する必要があります。

Oracleデータベースでサポートされるリストア処理のタイプ

SnapCenterでは、Oracleデータベースに対してさまざまなタイプのリストア処理を実行できます。

データベースをリストアする前に、バックアップが検証されて、実際のデータベース ファイルと比較して足りないファイルがないかが確認されます。

フル リストア

- データファイルのみをリストア
- 制御ファイルのみをリストア
- データファイルと制御ファイルをリストア
- Data GuardスタンバイとActive Data Guardスタンバイ データベースのデータファイル、制御ファイル、およびRedoログ ファイルをリストア

パーシャル リストア

- 選択した表領域のみをリストア
- 選択したPluggable Database (PDB) のみをリストア
- 1つのPDBの選択した表領域のみをリストア

Oracleデータベースでサポートされるリカバリ処理のタイプ

SnapCenterでは、Oracleデータベースに対してさまざまなタイプのリカバリ処理を実行できます。

- 最後のトランザクションまで（すべてのログ）のデータベース
- 特定のSystem Change Number (SCN) までのデータベース
- 特定の日時までのデータベース

リカバリの日時は、データベース ホストのタイムゾーンに基づいて指定する必要があります。

SnapCenterでは、Oracleデータベースに対して[No recovery]オプションも用意しています。



スタンバイとしてのデータベース ロールで作成されたバックアップを使用してリストアを行った場合、Plug-in for Oracle Databaseではリカバリがサポートされません。物理スタンバイ データベースは、常に手動でリカバリする必要があります。

Oracleデータベースのリストアとリカバリに関する制限事項

リストア処理とリカバリ処理を実行する前に、制限事項を確認しておく必要があります。

Oracle の 11.2.0.4 から 12.1.0.1 までのバージョンを使用している場合、*renamedg* コマンドを実行すると、復元操作がハング状態になります。この問題を修正するには、Oracleパッチ19544733を適用します。

次のリストア処理とリカバリ処理はサポートされていません。

- ルート コンテナ データベース (CDB) の表領域のリストアとリカバリ

- 一時表領域およびPDBに関連付けられた一時表領域のリストア
- 複数のPDBから同時に行う表領域のリストアとリカバリ
- ログ バックアップのリストア
- 別の場所へのバックアップのリストア
- Data GuardスタンバイまたはActive Data Guardスタンバイ データベース以外の構成でのRedoログ ファイルのリストア
- SPFILEおよびパスワード ファイルのリストア
- 同じホスト上に既存のデータベース名を使用して再作成され、SnapCenterで管理されていて、有効なバックアップがあるデータベースに対してリストア処理を実行すると、DBIDが異なる場合でも、新しく作成されたデータベース ファイルが上書きされます。

これを回避するには、次のいずれかの操作を実行します。

- データベースが再作成された後にSnapCenterリソースを検出する
- 再作成したデータベースのバックアップを作成する

表領域のポイントインタイム リカバリに関する制限事項

- SYSTEM、SYSAUX、およびUNDO表領域のポイントインタイム リカバリ（PITR）はサポートされていない
- 表領域のPITRを他のタイプのリストアと一緒に実行することはできない
- 名前が変更された表領域を、名前を変更する前の状態に戻す場合は、表領域の以前の名前を指定する必要がある
- ある表領域の表に対する制約が別の表領域に含まれている場合は、両方の表領域をリカバリする必要がある
- 表とそのインデックスが異なる表領域に格納されている場合は、PITRを実行する前にインデックスを削除する必要がある
- PITRを使用して、現在のデフォルト表領域をリカバリすることはできない
- 次のいずれかのオブジェクトを含む表領域は、PITRを使用してリカバリすることはできない：
 - 基礎となるオブジェクト（マテリアライズド・ビューなど）または含まれるオブジェクト（パーティション表など）を持つオブジェクト（ただし、基礎となるオブジェクトまたは含まれるオブジェクトのすべてがリカバリ・セットに含まれていない場合）

また、パーティション表のパーティションが異なる表領域に格納されている場合は、PITRを実行する前に表を削除するか、PITRを実行する前にすべてのパーティションを同じ表領域に移動する必要があります。

- セグメントを元に戻すまたはロールバックする
- 複数の受信者を持つ Oracle 8 互換の高度なキュー
- SYSユーザーが所有するオブジェクト

これらのタイプのオブジェクトの例としては、PL/SQL、Javaクラス、呼び出しプログラム、ビュー、シノニム、ユーザ、特権、ディメンション、ディレクトリ、シーケンスがあります。

Oracleデータベースのリストア処理のソースとデスティネーション

プライマリ ストレージまたはセカンダリ ストレージにあるバックアップ コピーからOracleデータベースをリストアすることができます。データベースは、同じデータベース インスタンスの同じ場所にしかリストアできません。ただし、Real Application Cluster (RAC) セットアップでは、データベースを他のノードにリストアできます。

リストア処理のソース

プライマリ ストレージまたはセカンダリ ストレージ上のバックアップからデータベースをリストアすることができます。複数ミラー構成でセカンダリ ストレージ上のバックアップからリストアする場合は、セカンダリ ストレージ ミラーをソースとして選択できます。

リストア処理のデスティネーション

データベースは、同じデータベース インスタンスの同じ場所にしかリストアできません。

RACセットアップでは、クラスタ内の任意のノードからRACデータベースをリストアできます。

リストア固有のプリスクリプトとポストスクリプト用に事前定義された環境変数

SnapCenterでは、データベースのリストア時にプリスクリプトとポストスクリプトを実行する際に、事前定義された環境変数を使用できます。

データベースの復元にサポートされている定義済み環境変数

- **SC_JOB_ID** は操作のジョブ ID を指定します。

例：257

- **SC_ORACLE_SID** はデータベースのシステム識別子を指定します。

複数のデータベースが処理対象となる場合、パイプで区切られたデータベース名が含まれます。

例：NFSB31

- **SC_HOST** はデータベースのホスト名を指定します。

このパラメータはアプリケーション ボリュームに対して設定されます。

例：scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** は、データベースのオペレーティング システムの所有者を指定します。

例：Oracle

- **SC_OS_GROUP** は、データベースのオペレーティング システム グループを指定します。

例：oinstall

- **SC_BACKUP_NAME** はバックアップの名前を指定します。

このパラメータはアプリケーション ボリュームに対して設定されます。

例:

- データベースがARCHIVELOGモードで実行されていない場合: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
- データベースが ARCHIVELOG モードで実行されている場合: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1, RG2_scspr2417819002_07-21-2021_12.16.48.9267_1, RG2_scspr2417819002_07-22-2021_12.16.48.9267_1

- **SC_BACKUP_ID** はバックアップの ID を指定します。

このパラメータはアプリケーション ボリュームに対して設定されます。

例:

- データベースがARCHIVELOGモードで実行されていない場合: DATA@203|LOG@205
- データベースがARCHIVELOGモードで実行されている場合: DATA@203|LOG@205,206,207

- **SC_RESOURCE_GROUP_NAME** はリソース グループの名前を指定します。

例: RG1

- **SC_ORACLE_HOME** は、Oracle ホーム ディレクトリのパスを指定します。

例: /ora01/app/oracle/product/18.1.0/db_1

- **SC_RECOVERY_TYPE** は、回復されるファイルと回復範囲を指定します。

例:

RESTORESCOPE:usingBackupControlfile=false|RECOVERYSCOPE:allLogs=true,noLogs=false,untiltime=false,untilscn=false。

区切り文字の詳細については、"[サポートされている区切り文字](#)"。

Oracleデータベースをリストアするための要件

Oracleデータベースをリストアする前に、前提条件が満たされていることを確認する必要があります。

- リストアとリカバリの戦略を定義しておく必要があります。
- ユーザがSnapshotをミラーまたはバックアップにレプリケートする場合は、ソース ボリュームとデスティネーション ボリューム両方のStorage Virtual Machine (SVM) をSnapCenter管理者がユーザに割り当てる必要があります。
- バックアップの一環としてアーカイブ ログが削除される場合は、必要なアーカイブ ログのバックアップを手動でマウントしておく必要があります。
- 仮想マシン ディスク (VMDK) 上にあるOracleデータベースをリストアする場合は、クローンVMDKを割り当てるための必要な数の空きスロットがゲスト マシンにあることを確認する必要があります。

- データベースでセカンダリ保護が有効になっている場合は、そのデータベースに属しているすべてのデータ ボリュームとアーカイブ ログ ボリュームが保護されていることを確認する必要があります。
- 制御ファイルまたはフル データベース リストアを実行するには、RAC One Nodeデータベースが「nomount」状態であることを確認する必要があります。
- NFS 環境に ASM データベース インスタンスがある場合は、リカバリ操作の一環として ASM ログ バックアップを正常にマウントするために、asm_diskstring パラメータで定義されている既存のパスに ASM ディスク パス `/var/opt/snapcenter/scu/clones/*/*` を追加する必要があります。
- asm_diskstring パラメータでは、ASMFD を使用している場合は `AFD:*` を構成し、ASMLIB を使用している場合は `ORCL:*` を構成する必要があります。



asm_diskstringパラメータを編集する方法については、以下を参照してください。
["asm_diskstringにディスクパスを追加する方法"](#)

- OS 認証を無効にし、Oracle データベースの Oracle データベース認証を有効にして、そのデータベースのデータファイルと制御ファイルを復元する場合は、非 ASM データベースの場合は `$ORACLE_HOME/network/admin`、ASM データベースの場合は `$GRID_HOME/network/admin` にある **listener.ora** ファイルで静的リスナーを構成する必要があります。
- データベース サイズがテラバイト (TB) 規模の場合は、Set-SmConfigSettingsコマンドを実行してSCORestoreTimeoutパラメータの値を増やす必要があります。
- vCenterに必要なすべてのライセンスがインストールされ、最新の状態になっていることを確認してください。

ライセンスがインストールされていないか最新の状態でない場合は、警告メッセージが表示されます。この警告を無視して続行すると、RDMからのリストアは失敗します。

- iSCSIプロトコルとFCプロトコルが混在するigroupを使用して、LUNがAIXホストにマッピングされていないことを確認します。詳細については、以下を参照してください。 ["LUNのデバイスを検出できないというエラーが発生し、操作が失敗しました"](#)。

Oracleデータベースのリストアとリカバリ

データ損失が発生した場合は、SnapCenterを使用して1つ以上のバックアップからアクティブ ファイルシステムにデータをリストアし、そのあとにデータベースをリカバリできます。

始める前に

root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプト ディレクトリとポストスクリプト ディレクトリに手動で割り当てる必要があります。

このタスクについて

- リカバリは、設定したアーカイブ ログの場所にあるアーカイブ ログを使用して実行されます。データベースがARCHIVELOGモードで実行されている場合、Redoログ ファイルでいっぱいになったグループは1つ以上のオフライン デスティネーション（総称：アーカイブRedoログ）に保存されます。SnapCenterは、指定したSCN、選択した日時、またはAll Logsオプションに基づいて、最適な数のログ バックアップを特定してマウントします。設定した場所にリカバリに必要なアーカイブ ログがない場合は、ログを含むSnapshotをマウントし、パスを外部アーカイブ ログとして指定する必要があります。

ASMデータベースをASMLIBからASMFDに移行する場合、ASMLIBで作成されたバックアップを使用してデータベースをリストアすることはできません。ASMFD設定でバックアップを作成し、リストアに使用する必要があります。同様に、ASMデータベースをASMFDからASMLIBに移行する場合は、リストアするバックアップをASMLIB設定で作成する必要があります。

データベースを復元すると、データベース上で複数の操作が実行されないように、Oracle データベースホストの `/var/opt/snapcenter/sco/lock` ディレクトリに操作ロック ファイル (`.sm_lock_dbsid`) が作成されます。処理ロック ファイルは、データベースのリストアが完了すると自動的に削除されます。



SPFILEおよびパスワード ファイルのリストアはサポートされていません。

- SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotのロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] または [リソース グループ] を選択します。
3. データベースの詳細ビューまたはリソース グループの詳細ビューでデータベースを選択します。

データベース トポロジのページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたは複製された) ストレージ システムから [バックアップ] を選択します。
5. 表からバックアップを選択し、*をクリックします。  *。
6. [Restore Scope] ページで、次の作業を実行します。

- a. Real Application Clusters (RAC) 環境でデータベースのバックアップを選択した場合は、RACノードを選択します。
- b. ミラー データまたはバックアップ データを選択する場合、以下のようになります。
 - ミラーまたはバックアップにログ バックアップが存在しない場合は、何も選択されず、ロケータは空になります。
 - ミラーまたはバックアップにログ バックアップが存在する場合は、最新のログ バックアップが選択され、対応するロケータが表示されます。



選択したログ バックアップがミラーとバックアップの両方の場所に存在する場合は、両方のロケータが表示されます。

- c. 次の操作を実行します。

リストアの対象	操作
データベースのすべてのデータファイル	*すべてのデータファイル*を選択します。 データベースのデータファイルのみがリストアされます。制御ファイル、アーカイブ ログ、Redo ログ ファイルはリストアされません。
Tablespaces	*表領域*を選択します。 リストアする表領域を指定できます。
Control files	*制御ファイル*を選択します。  制御ファイルをリストアするときは、リストア プロセスによってファイルがターゲットの場所にコピーされるように、ディレクトリ構造が存在することを確認します。必要に応じて、正しいユーザおよびグループの所有権が設定されたディレクトリ構造を作成する必要があります。ディレクトリが存在しない場合、リストア ジョブは失敗します。
Redo log files	*ログファイルを再実行*を選択します。 このオプションは、Data Guardスタンバイ データベースまたはActive Data Guardスタンバイ データベースでのみ選択できます。  Data Guard以外のデータベースのRedoログ ファイルはバックアップされません。Data Guard以外のデータベースでは、リカバリはアーカイブ ログを使用して実行されます。
Pluggable Database (PDB)	*プラグブル データベース*を選択し、復元する PDB を指定します。
プラグブルデータベース (PDB) 表領域	プラグブル データベース (PDB) 表領域 を選択し、復元する PDB とその PDB の表領域を指定します。 このオプションは、リストア対象にPDBを選択した場合にのみ選択できます。

- d. データベースの状態を復元および回復操作を実行するために必要な状態に変更するには、「復元および回復に必要な場合はデータベースの状態を変更する」を選択します。

データベースの状態には、高いレベルから順に、オープン、マウント済み、開始、シャットダウンがあります。リストア処理を実行するために、データベースの状態を高いレベルから低いレベルに変更する必要がある場合は、このチェック ボックスをオンにします。リストア処理を実行するために、データベースの状態を低いレベルから高いレベルに変更する必要がある場合は、このチェック ボックスをオンにしなくても自動的に状態が変更されます。

リストアのためにデータベースの状態をオープンからマウント済みに変更する必要がある場合は、このチェック ボックスをオンにした場合にのみデータベースの状態が変更されます。

- a. バックアップ後に新しいデータファイルが追加された場合や、LVM ディスク グループに LUN が追加、削除、または再作成された場合にインプレース リストアを実行する場合は、[強制インプレース リストア] を選択します。

7. [Recovery Scope] ページで、次の操作を実行します。

状況	操作
最後のトランザクションまでリカバリする場合	*すべてのログ*を選択します。
特定のSystem Change Number (SCN) までリカバリする場合	*SCN (システム変更番号) まで*を選択します。
特定の日時までリカバリする場合	*日付と時刻*を選択します。 データベース ホストのタイムゾーンの日付と時刻を指定する必要があります。
リカバリが不要である場合	*回復なし*を選択します。

状況	操作
外部アーカイブ ログの場所を指定する場合	データベースがARCHIVELOGモードで実行されている場合、SnapCenterは、指定したSCN、選択した日時、またはAll Logsオプションに基づいて、最適な数のログ バックアップを特定してマウントします。 外部アーカイブ ログ ファイルの場所を指定する場合は、[外部アーカイブ ログの場所を指定する] を選択します。 バックアップの一環としてアーカイブ ログが削除される場合に、必要なアーカイブ ログのバックアップを手動でマウントしたときは、リカバリのために、マウントしたバックアップのパスを外部アーカイブ ログの場所として指定する必要があります。  外部ログの場所としてリストする前に、マウント パスのパスと内容を確認する必要があります。 • "ONTAPによるOracleデータ保護" • "ORA-00308 エラーで操作が失敗しました"

アーカイブ ログ ボリュームが保護されておらず、データ ボリュームが保護されている場合は、セカンダリ バックアップからリカバリを伴うリストアを実行できません。**復元なし**を選択した場合にのみ復元できます。

[Open Database]オプションを選択してRACデータベースをリカバリする場合、リカバリ処理が開始されたRACインスタンスだけがオープン状態に戻ります。



Data GuardスタンバイおよびActive Data Guardスタンバイ データベースではリカバリがサポートされません。

8. [PreOps]ページで、リストア処理の前に実行するプリスクリプトのパスと引数を入力します。

プレスクリプトは、`/var/opt/snapcenter/spl/scripts` パスまたはこのパス内の任意のフォルダーに保存する必要があります。デフォルトでは、`/var/opt/snapcenter/spl/scripts` パスが設定されます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

スクリプトのタイムアウト値を指定することもできます。デフォルト値は60秒です。

SnapCenter、事前スクリプトと事後スクリプトを実行するときに、事前定義された環境変数を使用できます。["詳細情報"](#)

9. [PostOps]ページで、次の手順を実行します。

- a. リストア処理のあとに実行するポストスクリプトのパスと引数を入力します。

ポストスクリプトは、`/var/opt/snapcenter/spl/scripts` またはこのパス内の任意のフォルダーに保存する必要があります。デフォルトでは、`/var/opt/snapcenter/spl/scripts` パスが設定されます。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。



リストア処理が失敗した場合、ポストスクリプトは実行されず、クリーンアップ アクティビティが直接トリガーされます。

- b. リカバリ後にデータベースを開く場合は、チェック ボックスをオンにします。

リカバリ後にデータベースを開くように指定した場合は、制御ファイル付きまたは制御ファイルなしのコンテナ データベース (CDB) をリストアしたあと、またはCDB制御ファイルのみをリストアしたあとにCDBのみが開き、CDB内のPluggable Database (PDB) は開きません。

RACセットアップでは、リカバリに使用されるRACインスタンスのみがリカバリ後に開きます。



制御ファイル付きのユーザ表領域、制御ファイル付きまたは制御ファイルなしのシステム表領域、あるいは制御ファイル付きまたは制御ファイルなしのPDBをリストアすると、リストア処理に関連するPDBの状態のみが元の状態に変更されます。リストアに使用されなかった他のPDBの状態は保存されていないため、元の状態に変更されません。リストアに使用されなかったPDBの状態は、手動で変更する必要があります。

10. [通知] ページの [電子メール設定] ドロップダウン リストから、電子メール通知を送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。実行された復元操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択する必要があります。



Eメール通知を利用する場合は、GUIまたはPowerShellコマンドSet-SmSmtServerを使用して、SMTPサーバの詳細を指定しておく必要があります。

11. 概要を確認し、[完了] をクリックします。
12. モニター > ジョブ をクリックして、操作の進行状況を監視します。

詳細はこちら

- "Oracle RAC One NodeデータベースはSnapCenter操作の実行ではスキップされます"
- "セカンダリSnapMirrorまたはSnapVault の場所から復元できませんでした"
- "孤立したインカネーションのバックアップからの復元に失敗しました"
- "AIX システムでのバックアップ、復元、クローン操作のカスタマイズ可能なパラメータ"

ポイントインタイム リカバリを使用した表領域のリストアとリカバリ

破損または削除された表領域のサブセットは、データベース内の他の表領域に影響を与えることなくリストアできます。SnapCenterは、RMANを使用して表領域のポイントインタイムリカバリ (PITR) を実行します。

始める前に

- 表領域のPITRを実行するために必要なバックアップをカタログ化してマウントする必要があります。
- root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプト ディレクトリとポストスクリプト ディレクトリに手動で割り当てる必要があります。

このタスクについて

PITR処理中、RMANは指定された補助デスティネーションに補助インスタンスを作成します。補助デスティネーションには、マウント ポイントまたはASMディスク グループを指定できます。マウントされた場所に十分なスペースがある場合は、専用のマウント ポイントの代わりにいずれかのマウントされた場所を再利用できます。

日時またはSCNを指定すると、ソース データベースに表領域がリストアされます。

ASM、NFS、SAN環境にある複数の表領域を選択してリストアできます。たとえば、表領域TS2とTS3がNFS上にあり、TS4がSAN上にある場合、1回のPITR処理ですべての表領域をリストアできます。



RACセットアップでは、RACの任意のノードから表領域のPITRを実行できます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] または [リソース グループ] を選択します。
3. データベースの詳細ビューまたはリソース グループの詳細ビューで、タイプが単一インスタンス（マルチテナント）のデータベースを選択します。

データベース トポロジのページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたは複製された) ストレージ システムから [バックアップ] を選択します。

バックアップがカタログ化されていない場合は、バックアップを選択し、「カタログ」をクリックする必要があります。

5. カタログ化されたバックアップを選択し、*をクリックします。  *

6. [Restore Scope] ページで、次の作業を実行します。
 - a. Real Application Clusters (RAC) 環境でデータベースのバックアップを選択した場合は、RAC ノードを選択します。
 - b. *表領域*を選択し、復元する表領域を指定します。



SYSAUX、SYSTEM、UNDO表領域ではPITRを実行できません。

- c. データベースの状態を復元および回復操作を実行するために必要な状態に変更するには、「復元および回復に必要な場合はデータベースの状態を変更する」を選択します。
7. [Recovery Scope] ページで、次のいずれかを実行します。
 - 特定のシステム変更番号 (SCN) まで回復する場合は、「Until SCN」を選択し、SCN と補助宛先を指定します。

- ・ 特定の日付と時刻に復元する場合は、「日付と時刻」を選択し、日付と時刻および補助の宛先を指定します。

SnapCenterは、指定したSCNまたは選択した日時に基づいて、PITRの実行に必要なデータ バックアップとログ バックアップの最適な数を特定し、マウントしてカタログ化します。

8. [PreOps]ページで、リストア処理の前に実行するプリスクリプトのパスと引数を入力します。

プリスクリプトは、/var/opt/snapcenter/spl/scriptsパスまたはこのパス内の任意のフォルダに保存する必要があります。デフォルトでは、/var/opt/snapcenter/spl/scriptsがパスとして入力されています。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

スクリプトのタイムアウト値を指定することもできます。デフォルト値は60秒です。

SnapCenter、事前スクリプトと事後スクリプトを実行するときに、事前定義された環境変数を使用できます。["詳細情報"](#)

9. [PostOps]ページで、次の手順を実行します。

- a. リストア処理のあとに実行するポストスクリプトのパスと引数を入力します。



リストア処理が失敗した場合、ポストスクリプトは実行されず、クリーンアップ アクティビティが直接トリガーされます。

- b. リカバリ後にデータベースを開く場合は、チェック ボックスをオンにします。

10. [通知] ページの [電子メール設定] ドロップダウン リストから、電子メール通知を送信するシナリオを選択します。
11. 概要を確認し、[完了] をクリックします。
12. モニター > ジョブ をクリックして、操作の進行状況を監視します。

ポイントインタイム リカバリを使用したプラグブル データベースのリストアとリカバリ

破損または削除されたプラグブル データベース (PDB) は、コンテナ データベース (CDB) 内の他のPDBに影響を与えることなくリストアおよびリカバリできます。SnapCenterは、RMANを使用してPDBのポイントインタイム リカバリ (PITR) を実行します。

始める前に

- ・ PDBのPITRを実行するために必要なバックアップをカタログ化してマウントする必要があります。



RACセットアップでは、RACセットアップのすべてのノードでPDBを手動で閉じる (状態をマウント済みに変更する) 必要があります。

- ・ root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプト ディレクトリとポストスクリプト ディレクトリに手動で割り当てる必要があります。

このタスクについて

PITR処理中、RMANは指定された補助デスティネーションに補助インスタンスを作成します。補助デスティネーションには、マウント ポイントまたはASMディスク グループを指定できます。マウントされた場所に十分なスペースがある場合は、専用のマウント ポイントの代わりにいずれかのマウントされた場所を再利用できます。

PDBのPITRを実行するには、日時またはSCNを指定する必要があります。RMANは、読み取り / 書き込み、読み取り専用、またはデータファイルを含む削除されたPDBをリカバリできます。

リストアとリカバリには、以下の制限があります。

- 一度に1つのPDB
- PDB内の1つの表領域
- 同じPDBの複数の表領域



RACセットアップでは、RACの任意のノードから表領域のPITRを実行できます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] または [リソース グループ] を選択します。
3. データベースの詳細ビューまたはリソース グループの詳細ビューで、タイプが単一インスタンス（マルチテナント）のデータベースを選択します。

データベース トポロジのページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたは複製された) ストレージ システムから [バックアップ] を選択します。

バックアップがカタログ化されていない場合は、バックアップを選択し、「カタログ」をクリックする必要があります。

5. カタログ化されたバックアップを選択し、*をクリックします。*。

6. [Restore Scope] ページで、次の作業を実行します。
 - a. Real Application Clusters（RAC）環境でデータベースのバックアップを選択した場合は、RACノードを選択します。
 - b. PDBとPDB内の表領域のどちらをリストアするかに応じて、次のいずれかの操作を実行します。

状況	手順
PDBをリストアする	i. プラガブル データベース (PDB) を選択します。 ii. リストアするPDBを指定します。  PDB\$SEEDデータベースではPITRを実行できません。

PDB内の表領域をリストアする	i. プラガブル データベース (PDB) 表領域 を選択します。 ii. PDBを指定します。 iii. リストアする表領域を1つまたは複数指定します。  SYSAUX、SYSTEM、UNDO 表領域ではPITRを実行できません。

- c. データベースの状態を復元および回復操作を実行するために必要な状態に変更するには、「復元および回復に必要な場合はデータベースの状態を変更する」を選択します。

7. [Recovery Scope]ページで、次のいずれかを実行します。

- 特定のシステム変更番号 (SCN) まで回復する場合は、「**Until SCN**」を選択し、SCN と補助宛先を指定します。
- 特定の日付と時刻に復元する場合は、「日付と時刻」を選択し、日付と時刻および補助の宛先を指定します。

SnapCenterは、指定したSCNまたは選択した日時に基づいて、PITRの実行に必要なデータ バックアップとログ バックアップの最適な数を特定し、マウントしてカタログ化します。

8. [PreOps]ページで、リストア処理の前に実行するプリスクリプトのパスと引数を入力します。

プリスクリプトは、/var/opt/snapcenter/spl/scriptsパスまたはこのパス内の任意のフォルダに保存する必要があります。デフォルトでは、/var/opt/snapcenter/spl/scriptsがパスとして入力されています。スクリプトを保存するフォルダをこのパス内に作成してある場合は、パス内のそれらのフォルダを指定する必要があります。

スクリプトのタイムアウト値を指定することもできます。デフォルト値は60秒です。

SnapCenter、事前スクリプトと事後スクリプトを実行するときに、事前定義された環境変数を使用できます。["詳細情報"](#)

9. [PostOps]ページで、次の手順を実行します。

- a. リストア処理のあとに実行するポストスクリプトのパスと引数を入力します。



リストア処理が失敗した場合、ポストスクリプトは実行されず、クリーンアップ アクティビティが直接トリガーされます。

- b. リカバリ後にデータベースを開く場合は、チェック ボックスをオンにします。

RACセットアップでは、データベースがリカバリされたノードでのみPDBが開きます。リカバリしたPDBは、RACセットアップの他のすべてのノードで手動で開く必要があります。

10. [通知] ページの [電子メール設定] ドロップダウン リストから、電子メール通知を送信するシナリオを選択します。

11. 概要を確認し、[完了] をクリックします。
12. モニター > ジョブ をクリックして、操作の進行状況を監視します。

UNIXコマンドを使用したOracleデータベースのリストアとリカバリ

リストアとリカバリのワークフローには、計画、リストア処理とリカバリ処理の実行、および処理の監視が含まれます。

このタスクについて

- 次の各コマンドを実行して、SnapCenter Serverとの接続を確立し、バックアップをリストしてその情報を取得し、バックアップをリストアする必要があります。

コマンドで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンド リファレンス ガイド](#)"。

- SnapMirrorアクティブ同期でリストア処理を実行するには、プライマリの場所からバックアップを選択する必要があります。

手順

1. 指定されたユーザーのSnapCenter Server との接続セッションを開始します: *Open-SmConnection*
2. 復元するバックアップに関する情報を取得します: *Get-SmBackup*
3. 指定されたバックアップの詳細情報を取得します: *Get-SmBackupDetails*

このコマンドでは、バックアップIDで指定された特定のリソースのバックアップに関する詳細情報を取得します。取得される情報には、データベースの名前、バージョン、ホーム、開始SCNと終了SCN、表領域、Pluggable Databaseとその表領域などがあります。

4. バックアップからデータを復元する: *Restore-SmBackup*

Oracleデータベースのリストア処理の監視

[Job]ページを使用して、SnapCenterの各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-

 警告付きで完了したか、警告のため開始できませんでした

-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター* ページで、*ジョブ* をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  てリストをフィルタリングし、リストア処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ* ドロップダウンリストから*復元*を選択します。
 - d. *ステータス* ドロップダウンリストから、復元ステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. 復元ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細* ページで、*ログの表示* をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

Oracle データベースのリストア処理のキャンセル

キューに登録されているリストア ジョブはキャンセルできます。

リストア処理をキャンセルするには、SnapCenter 管理者がジョブ所有者としてログインする必要があります。

タスク概要

- キューに入れられた復元操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のリストア処理はキャンセルできません。
- キューに登録されているリストア処理のキャンセルには、SnapCenter GUI、PowerShell コマンドレット、または CLI コマンドを使用できます。
- キャンセルできない復元操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられた復元操作をキャンセルできます。

手順

次のいずれかを実行します。

方法	アクション
[Monitor]ページ	1. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 2. ジョブを選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	1. 復元操作を開始したら、 アクティビティ ペインで、最新の 5 つの操作を表示します。 2. 処理を選択します。 3. ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

Oracle データベースのクローニング

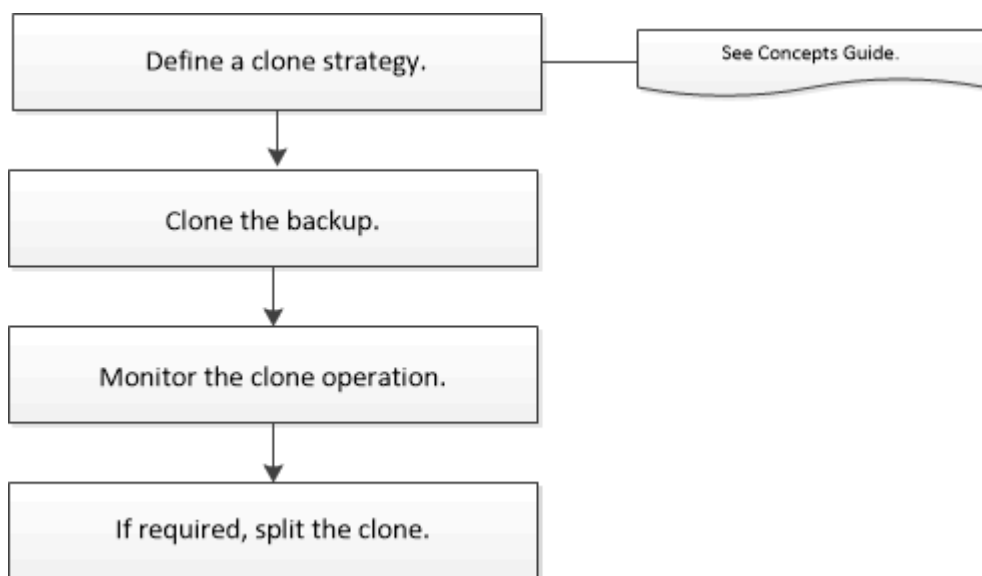
クローニングのワークフロー

クローニング ワークフローには、計画、クローニング処理の実行、および処理の監視が含まれます。

データベースをクローニングする理由には次のものがあります。

- アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のデータベースの構造およびコンテナツを使用してテストするため。
- データの抽出と操作を行うツールを使用してデータ ウェアハウスにデータを取り込むため。
- 誤って削除または変更されたデータをリカバリするため。

次のワークフローは、クローニング処理の実行順序を示しています。



Oracleデータベースのクローニング戦略の定義

データベースをクローニングする前に戦略を定義しておく、クローニング処理を確実に成功させることができます。

クローニングでサポートされるバックアップのタイプ

SnapCenterでは、Oracleデータベースの各種バックアップのクローニングがサポートされます。

- オンライン データ バックアップ
- オンライン フル バックアップ
- オフライン マウント バックアップ
- オフライン シャットダウン バックアップ
- Data Guardスタンバイ データベースおよびActive Data Guardスタンバイ データベースのバックアップ
- Real Application Clusters (RAC) 構成でのオンライン データ バックアップ、オンライン フル バックアップ、オフライン マウント バックアップ、オフライン シャットダウン バックアップ
- Automatic Storage Management (ASM) 構成でのオンライン データ バックアップ、オンライン フル バックアップ、オフライン マウント バックアップ、オフライン シャットダウン バックアップ



マルチパス構成ファイルのuser_friendly_namesオプションがyesに設定されている場合、SAN構成はサポートされません。



アーカイブ ログ バックアップのクローニングはサポートされていません。

Oracleデータベースでサポートされるクローニングのタイプ

Oracle データベース環境では、SnapCenter はデータベース バックアップのクローン作成をサポートします。バックアップのクローニングは、プライマリ ストレージ システムおよびセカンダリ ストレージ システムから行うことができます。

SnapCenter Server は、NetApp FlexCloneテクノロジーを使用してバックアップを複製します。

クローンを更新するには、「Refresh-SmClone」コマンドを実行します。このコマンドを実行すると、データベースのバックアップが作成され、既存のクローンは削除され、同じ名前のクローンが作成されます。



クローンの更新処理は、UNIXコマンドを使わないと実行できません。

Oracleデータベースのクローンの命名規則

SnapCenter 3.0 以降、ファイル システムのクローンに対して使用される命名規則は、ASM ディスク グループのクローンに対して使用される命名規則とは異なります。

- SANファイルシステムまたはNFSファイルシステムの命名規則は、FileSystemNameofsourcedatabase_CLONESIDです。
- ASMディスク グループの命名規則は、SC_HASHCODEofDISKGROUP_CLONESIDです。

HASHCODEofDISKGROUPは、自動生成される2～10桁の数値で、各ASMディスク グループに固有です。

Oracleデータベースのクローニングに関する制限事項

データベースをクローニングする前に、クローニング処理の制限事項を確認しておく必要があります。

- Oracle の 11.2.0.4 から 12.1.0.1 までのバージョンを使用している場合、*renamedg* コマンドを実行するとクローン操作がハング状態になります。この問題を修正するには、Oracleパッチ19544733を適用します。
- (WindowsホストでMicrosoft iSCSIイニシエータを使用するなどして) ホストに直接接続されているLUNから、同じWindowsホスト上のVMDKかRDM LUN、または別のWindowsホストにデータベースをクローニングすることはできません。その逆も同様です。
- ボリューム マウント ポイントのルート ディレクトリを共有ディレクトリにすることはできません。
- クローンを含むLUNを新しいボリュームに移動すると、そのクローンは削除できなくなります。

クローン固有のプリスクリプトとポストスクリプト用に事前定義された環境変数

SnapCenterでは、データベースのクローニング時にプリスクリプトとポストスクリプトを実行する際に、事前定義された環境変数を使用できます。

データベースのクローン作成にサポートされている定義済み環境変数

- **SC_ORIGINAL_SID** は、ソース データベースの SID を指定します。

このパラメータはアプリケーション ボリュームに対して設定されます。

例：NFSB32

- **SC_ORIGINAL_HOST** は、ソース ホストの名前を指定します。

このパラメータはアプリケーション ボリュームに対して設定されます。

例：asmrac1.gdl.englab.netapp.com

- **SC_ORACLE_HOME** は、ターゲット データベースの Oracle ホーム ディレクトリのパスを指定します。

例: /ora01/app/oracle/product/18.1.0/db_1

- **SC_BACKUP_NAME** はバックアップの名前を指定します。

このパラメータはアプリケーション ボリュームに対して設定されます。

例:

- データベースがARCHIVELOGモードで実行されていない場合: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
- データベースが ARCHIVELOG モードで実行されている場合: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG:RG2_scspr2417819002_07-20-2021_12.16.48.9267_1,RG2_scspr2417819002_07-21-

- **SC_AV_NAME** はアプリケーション ボリュームの名前を指定します。

例: AV1|AV2

- **SC_ORIGINAL_OS_USER** は、ソース データベースのオペレーティング システムの所有者を指定します。

例: Oracle

- **SC_ORIGINAL_OS_GROUP** は、ソース データベースのオペレーティング システム グループを指定します。

例: oinstall

- **SC_TARGET_SID** は、クローンされたデータベースの SID を指定します。

PDBクローン ワークフローの場合、このパラメータの値は事前定義されません。

このパラメータはアプリケーション ボリュームに対して設定されます。

例: clonedb

- **SC_TARGET_HOST** は、データベースのクローンが作成されるホストの名前を指定します。

このパラメータはアプリケーション ボリュームに対して設定されます。

例: asmrac1.gdl.englab.netapp.com

- **SC_TARGET_OS_USER** は、クローンされたデータベースのオペレーティング システムの所有者を指定します。

PDBクローン ワークフローの場合、このパラメータの値は事前定義されません。

例: Oracle

- **SC_TARGET_OS_GROUP** は、クローンされたデータベースのオペレーティング システム グループを指定します。

PDBクローン ワークフローの場合、このパラメータの値は事前定義されません。

例: oinstall

- **SC_TARGET_DB_PORT** は、クローンされたデータベースのデータベース ポートを指定します。

PDBクローン ワークフローの場合、このパラメータの値は事前定義されません。

例: 1521

区切り文字の詳細については、"[サポートされている区切り文字](#)"。

Oracleデータベースをクローニングするための要件

Oracleデータベースをクローニングする前に、前提条件が満たされていることを確認する必要があります。

- SnapCenterを使用してデータベースのバックアップを作成しておく必要があります。

クローニング処理を行うには、オンラインのデータ バックアップとログのバックアップ、またはオフラインでの（マウントまたはシャットダウンの）バックアップが正常に作成されている必要があります。

- 制御ファイルまたはRedoログ ファイルのパスをカスタマイズする場合は、必要なファイルシステムまたはAutomatic Storage Management (ASM) ディスク グループを事前にプロビジョニングしておく必要があります。

デフォルトでは、クローン データベースのRedoログ ファイルと制御ファイルは、クローン データベースのデータ ファイル用にSnapCenterによってプロビジョニングされたASMディスク グループまたはファイルシステムに作成されます。

- NFS 経由で ASM を使用している場合は、asm_diskstring パラメータで定義されている既存のパスに `/var/opt/snapcenter/scu/clones/*/*` を追加する必要があります。
- asm_diskstring パラメータでは、ASMFD を使用している場合は `AFD:*` を構成し、ASMLIB を使用している場合は `ORCL:*` を構成する必要があります。

asm_diskstringパラメータを編集する方法については、以下を参照してください。 ["asm_diskstringにディスクパスを追加する方法"](#)。

- 代替ホストにクローンを作成する場合は、代替ホストが次の要件を満たしている必要があります。
 - 代替ホストにSnapCenter Plug-in for Oracle Database をインストールする必要があります。
 - クローン ホストは、プライマリ ストレージまたはセカンダリ ストレージから LUN を検出する必要があります。
 - プライマリ ストレージまたはセカンダリ (Vault または Mirror) ストレージから代替ホストにクローンを作成する場合は、セカンダリ ストレージと代替ホストの間で iSCSI セッションが確立されていること、または FC 用に適切にゾーン分けされていることを確認します。
 - Vault またはミラー ストレージから同じホストにクローンを作成する場合は、Vault またはミラー ストレージとホストの間で iSCSI セッションが確立されていること、または FC 用に適切にゾーン分けされていることを確認してください。
 - 仮想化環境でクローンを作成する場合は、プライマリまたはセカンダリ ストレージと代替ホストをホストする ESX サーバーの間で iSCSI セッションが確立されていること、または FC 用に適切にゾーン分けされていることを確認します。

詳細については、 ["ホストユーティリティのドキュメント"](#)。

- ソース データベースが ASM データベースの場合:
 - クローンが実行されるホスト上で ASM インスタンスが起動され、実行されている必要があります。
 - クローンされたデータベースのアーカイブ ログ ファイルを専用の ASM ディスク グループに配置する場合は、クローン操作の前に ASM ディスク グループをプロビジョニングする必要があります。

- データ ディスク グループの名前は構成できますが、クローンが実行されるホスト上の他の ASM ディスク グループでその名前が使用されていないことを確認してください。

ASM ディスク グループ上のデータ ファイルは、SnapCenter クローン ワークフローの一部としてプロビジョニングされます。

◦ NVMe の場合は、NVMe ユーティリティがインストールされている必要があります。

- ログ バックアップを使用した代替ホストへのクローニングの際にセカンダリ ロケータを検出するには、データ LUN とログ LUN の保護タイプ (mirror、vault、mirror-vault など) を同じものにする必要があります。
- 12_c_ データベースのバックアップをクローンするためのシード PDB 関連情報を取得するには、ソース データベース パラメータ ファイルで `exclude_seed_cdb_view` の値を `FALSE` に設定する必要があります。

シード PDB とは、CDB が PDB を作成する際に使用する、システム付属のテンプレートです。シード PDB の名前は `PDB$SEED` です。PDB\$SEED については、Oracle Doc ID 1940806.1 を参照してください。



12_c_ データベースをバックアップする前に値を設定する必要があります。

- SnapCenter は autofs サブシステムによって管理されるファイルシステムのバックアップをサポートしています。データベースをクローニングする場合は、データ マウント ポイントが autofs マウント ポイントのルートの下に配置されないようにしてください。プラグイン ホストの root ユーザには、autofs マウント ポイントのルートの下にディレクトリを作成する権限がないためです。

制御ログ ファイルと Redo ログ ファイルがデータ マウント ポイントにある場合は、制御ファイルのパスを変更し、Redo ログ ファイルのパスも適切に変更する必要があります。



クローニングされた新しいマウント ポイントは autofs サブシステムに手動で登録できません。クローニングされた新しいマウント ポイントが自動的に登録されることはありません。

- TDE (自動ログイン) があり、同じホストまたは別のホストにデータベースを複製する場合は、`/etc/ORACLE/WALLET/$ORACLE_SID` の下にあるウォレット (キー ファイル) をソース データベースから複製されたデータベースにコピーする必要があります。
- Oracle Linux 7 以降または Red Hat Enterprise Linux (RHEL) 7 以降のストレージ エリア ネットワーク (SAN) 環境でクローン作成を正常に実行するには、`/etc/lvm/lvm.conf` で `use_lvmetad = 0` の値を設定し、`lvm2-lvmetad` サービスを停止する必要があります。
- Oracle データベース 11.2.0.3 以降を使用していて、補助インスタンスのデータベース ID が NID スクリプトを使用して変更されている場合は、13366202 Oracle パッチをインストールする必要があります。
- ボリュームをホストするアグリゲートが Storage Virtual Machine (SVM) の割り当て済みアグリゲート リストに含まれていることを確認します。
- NVMe で接続から除外する必要があるターゲット ポートがある場合は、ターゲットのノード名とポート名を `/var/opt/snapcenter/scu/etc/nvme.conf` ファイルに追加します。

ファイルが存在しない場合は、次の例に示すようにファイルを作成する必要があります。

```
blacklist {
nn-0x<target_node_name_1>:pn-0x<target_port_name_1>
nn-0x<target_node_name_2>:pn-0x<target_port_name_2>
}
```

- iSCSIプロトコルとFCプロトコルが混在するigroupを使用して、LUNがAIXホストにマッピングされていないことを確認します。詳細については、以下を参照してください。"[LUNのデバイスを検出できないというエラーが発生し、操作が失敗しました](#)"。

Oracleデータベース バックアップのクローニング

SnapCenterを使用すると、データベースのバックアップ機能でOracleデータベースをクローニングできます。

始める前に

root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプト ディレクトリとポストスクリプト ディレクトリに手動で割り当てる必要があります。

このタスクについて

- クローニング処理では、データベースのデータ ファイルのコピーが作成され、新しいオンラインRedoログ ファイルと制御ファイルが作成されます。データベースは、指定したリカバリ オプションに基づいて、指定した時間にリカバリすることもできます。



Linuxホストで作成されたバックアップをAIXホストにクローニングしようとする、クローニングは失敗します。逆の場合も同様です。

SnapCenterでは、Oracle RACデータベース バックアップからクローニングすると、スタンドアロン データベースが作成されます。SnapCenterでは、Data Guardスタンバイ データベースおよびActive Data Guardスタンバイ データベースのバックアップからのクローンの作成がサポートされています。

クローニング中、SnapCenterでは、リカバリ処理のSCNまたは日時に基づいて、最適な数のログ バックアップがマウントされます。リカバリが完了すると、ログ バックアップはアンマウントされます。このようなクローンすべては、`/var/opt/snapcenter/scu/clones/`の下にマウントされます。NFS 経由でASM を使用している場合は、`asm_diskstring` パラメータで定義されている既存のパスに `/var/opt/snapcenter/scu/clones/*/*` を追加する必要があります。

SAN 環境でASM データベースのバックアップをクローン作成するときに、クローン作成されたホスト デバイスのudev ルールが `/etc/udev/rules.d/999-scu-netapp.rules` に作成されます。クローニングされるホスト デバイスに関連付けられたudevルールは、クローンを削除すると削除されます。



Flex ASMセットアップでは、カーディナリティがRACクラスタ内のノード数より少ない場合、リーフ ノードではクローニング処理を実行できません。

- SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotのロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] または [リソース グループ] を選択します。
3. データベースの詳細ビューまたはリソース グループの詳細ビューでデータベースを選択します。

データベース トポロジのページが表示されます。

4. [Manage Copies]ビューで、ローカル コピー（プライマリ）、ミラー コピー（セカンダリ）、バックアップ コピー（セカンダリ）のいずれかのバックアップを選択します。
5. 表からデータバックアップを選択し、*をクリックします。  *。
6. [Name]ページで、次のいずれかを実行します。

状況	手順
データベースのクローニング（CDBまたは非CDB）	a. クローンのSIDを指定します。 クローンSIDはデフォルトでは使用できず、SIDの最大長は8文字です。  クローンが作成されるホストに、同じSIDのデータベースが存在しないことを確認してください。
プラガブル データベース（PDB）のクローニング	a. *PDB クローン*を選択します。 b. クローニングするPDBを指定します。 c. クローニングされたPDBの名前を指定します。PDBのクローンを作成する詳細な手順については、"プラガブル データベースのクローニング"。

ミラー データまたはバックアップ データを選択する場合、以下のようになります。

- ミラーまたはバックアップにログ バックアップが存在しない場合は、何も選択されず、ロケータは空になります。
- ミラーまたはバックアップにログ バックアップが存在する場合は、最新のログ バックアップが選択され、対応するロケータが表示されます。



選択したログ バックアップがミラーとバックアップの両方の場所に存在する場合は、両方のロケータが表示されます。

7. [Locations]ページで、次の操作を実行します。

フィールド	操作
Clone host	ソース データベース ホストがデフォルトで入力されています。 代替ホストにクローンを作成する場合は、ソース データベース ホストと同じバージョンのOracleおよびOSがインストールされているホストを選択します。
Datafile locations	データ ファイルの場所がデフォルトで入力されています。 SANファイルシステムまたはNFSファイルシステムのSnapCenterのデフォルトの命名規則は、FileSystemNameofsourcedatabase_CLONESIDです。 SnapCenterで設定されているASMディスク グループのデフォルトの命名規則は、SC_HASHCODEofDISKGROUP_CLONESIDです。HASHCODEofDISKGROUPは、自動生成される2～10桁の数値で、各ASMディスク グループに固有です。  ASMディスク グループ名をカスタマイズする場合は、名前の長さがOracleでサポートされる最大長に準拠していることを確認してください。 別のパスを指定する場合は、クローン データベースのデータファイル マウント ポイントまたはASMディスク グループ名を入力する必要があります。データ ファイル パスをカスタマイズする場合は、制御ファイルおよびRedoログ ファイルのASMディスク グループ名またはファイルシステムも、データ ファイルに使用されているのと同じ名前か、既存のASMディスク グループまたはファイルシステムに変更する必要があります。

フィールド	操作
Control files	制御ファイルのパスがデフォルトで入力されています。 制御ファイルは、データ ファイルと同じASMディスク グループまたはファイルシステムに配置されます。制御ファイルのパスは、別の制御ファイルのパスを指定して上書きできます。  ファイルシステムまたはASMディスク グループがホストに存在する必要があります。 デフォルトでは、制御ファイルの数はソース データベースの数と同じです。制御ファイルの数は変更できますが、データベースをクローニングするには少なくとも1つの制御ファイルが必要です。 制御ファイルのパスは、ソース データベースで設定したものとは別のファイルシステム（既存のファイルシステム）にカスタマイズできます。

フィールド	操作
Redo logs	redoログ ファイル グループ、パス、およびサイズがデフォルトで入力されています。 Redoログは、クローン データベースのデータ ファイルと同じASMディスク グループまたはファイル システムに配置されます。Redoログ ファイルのパスを上書きする場合は、Redoログ ファイルのパスをソース データベースで設定したものとは別のファイルシステムにカスタマイズできます。  新しいファイルシステムまたはASM ディスク グループがホストに存在している必要があります。 デフォルトでは、Redoログ グループとRedoログ ファイルの数とサイズはソース データベースと同じです。次のパラメータを変更できます。 • REDOロググループの数  データベースをクローニングするには、少なくとも2つのRedoログ グループが必要です。 • 各グループ内のREDOログファイルとそのパス Redoログ ファイルのパスは、ソース データベースで設定したものとは別のファイルシステム（既存のファイルシステム）にカスタマイズできます。  データベースをクローニングするには、Redoログ グループに少なくとも1つのRedoログ ファイルが必要です。 • REDOログファイルのサイズ

8. [Credentials]ページで、次の操作を実行します。

フィールド	操作
sysユーザーの資格情報名	クローン データベースの sys ユーザ パスワードの定義に使用するクレデンシャルを選択します。 ターゲット ホストの sqlnet.ora ファイルで SQLNET.AUTHENTICATION_SERVICES が NONE に設定されている場合、 SnapCenter GUI で資格情報として None を選択しないでください。
ASM Instance Credential name	クローン ホスト上の ASM インスタンスに接続するために OS 認証が有効になっている場合は、[なし]を選択します。 それ以外の場合は、「sys」ユーザーまたはクローン ホストに適用可能な「sysasm」権限を持つユーザーで構成された Oracle ASM 資格情報を選択します。

Oracleホーム、ユーザ名、およびグループの詳細が、ソース データベースから自動的に入力されます。値は、クローンが作成されるホストのOracle環境に基づいて変更できます。

9. [PreOps]ページで、次の手順を実行します。

- a. クローニング処理の前に実行するプリスクリプトのパスと引数を入力します。

プレスクリプトは、`/var/opt/snapcenter/spl/scripts` またはこのパス内の任意のフォルダーに保存する必要があります。デフォルトでは、`/var/opt/snapcenter/spl/scripts` パスが設定されます。スクリプトをこのパス内の任意のフォルダに配置した場合は、スクリプトの配置先となるフォルダまでの完全なパスを指定する必要があります。

SnapCenter、事前スクリプトと事後スクリプトを実行するときに、事前定義された環境変数を使用できます。["詳細情報"](#)

- b. [Database Parameter settings]セクションで、データベースの初期化に使用される事前入力されたデータベース パラメータの値を変更します。

をクリックすると追加のパラメータを追加できます 。

Oracle Standard Editionを使用しており、データベースがアーカイブ ログ モードで実行されている場合、またはアーカイブRedoログからデータベースをリストアする場合は、パラメータを追加してパスを指定します。

- ログアーカイブ先
- ログ_アーカイブ_デュプレックス_宛先



入力済みのデータベース パラメータでは、高速リカバリ領域（FRA）は定義されていません。FRAを設定するには、関連パラメータを追加します。



log_archive_dest_1のデフォルト値は\$ORACLE_HOME/clone_sidで、この場所にクローンデータベースのアーカイブ ログが作成されます。log_archive_dest_1パラメータを削除した場合は、Oracleによってアーカイブ ログの場所が決定されます。Log_archive_dest_1を編集することでアーカイブ ログの新しい場所を定義できますが、その際はファイルシステムまたはディスク グループが存在し、ホスト上で使用可能になっていることを確認してください。

a. *リセット*をクリックすると、デフォルトのデータベース パラメータ設定が取得されます。

10. PostOps ページでは、クローンされたデータベースの回復を実行するために、データベースの回復 と キャンセルまで がデフォルトで選択されています。

SnapCenterは、クローニング対象として選択されたデータ バックアップのあとに、破損していない一連のアーカイブ ログを含む最新のログ バックアップをマウントすることでリカバリを実行します。プライマリ ストレージでクローニングを実行するには、ログとデータのバックアップをプライマリ ストレージに配置し、セカンダリ ストレージでクローニングを実行するには、ログとデータのバックアップをセカンダリ ストレージに配置する必要があります。

SnapCenter が適切なログ バックアップを見つけられない場合は、データベースの回復 および キャンセルまで オプションは選択されません。*外部アーカイブ ログの場所の指定*でログ バックアップが利用できない場合は、外部アーカイブ ログの場所を指定できます。ログの場所は複数指定できます。



フラッシュ リカバリ領域（FRA）とOracle Managed Files（OMF）をサポートするように設定されているソース データベースをクローニングする場合は、リカバリのログ デステーションもOMFディレクトリ構造に従っている必要があります。

ソース データベースがData Guardスタンバイ データベースまたはActive Data Guardスタンバイ データベースの場合、[PostOps]ページは表示されません。Data Guardスタンバイ データベースまたはActive Data Guardスタンバイ データベースの場合、SnapCenterにはSnapCenter GUIでリカバリ タイプを選択するオプションはありませんが、ログを適用せずに[Cancel]リカバリ タイプを使用してデータベースをリカバリします。

フィールド名	説明
キャンセルまで	SnapCenterは、クローニング対象として選択されたデータ バックアップのあとに、破損していない一連のアーカイブ ログを含む最新のログ バックアップをマウントすることでリカバリを実行します。クローン データベースは、欠落または破損したログ ファイルまでリカバリされます。
Date and time	SnapCenterは、指定された日時までデータベースをリカバリします。有効な形式はmm/dd/yyyy hh:mm:ssです。  時刻は24時間形式で指定できます。
Until SCN (System Change Number)	SnapCenterは、指定されたシステム変更番号（SCN）までデータベースをリカバリします。

フィールド名	説明
Specify external archive log locations	データベースがARCHIVELOGモードで実行されている場合、SnapCenterは指定したSCNまたは選択した日時に基づいて、最適な数のログ バックアップを識別してマウントします。 外部アーカイブ ログの場所を指定することもできます。  [Until Cancel]を選択した場合、SnapCenterがログ バックアップを自動的に識別してマウントすることはありません。
新しいDBIDを作成する	デフォルトでは、新しい DBID の作成 チェックボックスが選択されており、クローンされたデータベースとソース データベースを区別する一意の番号 (DBID) が生成されます。 ソース データベースのDBIDをクローン データベースに割り当てる場合は、このチェック ボックスをオフにします。このシナリオでは、ソース データベースがすでに登録されている外部のRMANカタログにクローン データベースを登録すると、処理は失敗します。
一時表領域用の一時ファイルを作成する	クローン データベースのデフォルトの一時表領域用の一時ファイルを作成する場合は、このチェックボックスを選択します。 このチェック ボックスをオフにすると、一時ファイルなしでデータベース クローンが作成されます。
Enter sql entries to apply when clone is created	クローンの作成時に適用するSQLエントリを追加します。

フィールド名	説明
Enter scripts to run after clone operation	クローニング処理のあとに実行するポストスクリプトのパスと引数を指定します。 ポストスクリプトは、<code>/var/opt/snapcenter/spl/scripts</code> またはこのパス内の任意のフォルダーに保存する必要があります。デフォルトでは、<code>/var/opt/snapcenter/spl/scripts</code> パスが設定されます。 スクリプトをこのパス内の任意のフォルダに配置した場合は、スクリプトの配置先となるフォルダまでの完全なパスを指定する必要があります。  クローニング処理が失敗した場合、ポストスクリプトは実行されず、クリーンアップ アクティビティが直接トリガーされます。

11. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。実行されたクローン操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

12. 概要を確認し、[完了] をクリックします。



クローニング処理の一環としてリカバリを実行する場合は、リカバリが失敗してもクローンが作成され、警告が表示されます。このクローンに対して手動リカバリを実行することで、クローン データベースの整合性を確保できます。

13. モニター > ジョブ をクリックして、操作の進行状況を監視します。

結果

データベースをクローニングしたあとにリソース ページを更新すると、クローン データベースが、バックアップ対象のリソースの1つとしてリストに追加されます。クローニングされたデータベースは、標準のバックアップ ワークフローを使用して他のデータベースと同様に保護することも、リソース グループ（新規または既存）に含めることもできます。クローニングされたデータベースは、さらにクローニングすることができます（クローンのクローン）。

クローニング後は、クローン データベースの名前を変更しないでください。



クローニング中にリカバリを実行しなかった場合は、不適切なリカバリが原因でクローン データベースのバックアップが失敗して、手動でのリカバリが必要になることがあります。また、アーカイブ ログ用に設定されていたデフォルトの場所がNetApp以外のストレージにある場合や、ストレージ システムでSnapCenterが設定されていない場合も、ログのバックアップは失敗することがあります。

AIXのセットアップでは、lkdevコマンドを使用して、クローン データベースが配置されているディスクをロックし、rendevコマンドを使用してディスク名を変更することができます。

デバイスをロックまたは名前変更しても、クローンの削除処理には影響しません。SANデバイス上に構築されたAIX LVMレイアウトでは、クローニングされたSANデバイスのデバイス名の変更はサポートされません。

詳細情報

- "ORA-00308 エラーメッセージが表示され、復元またはクローン作成が失敗する"
- "クローンデータベースの回復に失敗しました"
- "AIX システムでのバックアップ、復元、クローン操作のカスタマイズ可能なパラメータ"

ホストの優先IPを更新する

クローン操作が完了すると、ストレージ アクセス レイヤー (SAL) によってクローンに提供されるパスは、<nfs_lif_IP>:<JunctionPath> 形式になります。優先 IP を提供するには、SCCLI コマンドを使用してホスト上で設定する必要があります。

手順

1. データベース ホストにログインします。
2. 指定されたユーザーに対して、SnapCenterとの PowerShell 接続セッションを開始します。

```
Open-SmConnection
```

3. 空のファイルを作成します。

```
/var/opt/snapcenter/scu/etc/storagepreference.properties をタッチします。
```

4. SVM の優先データ LIF を設定します。

```
Add-SvmPreferredDataPath -SVM <SVM 名> -DataPath <IP アドレスまたは FQDN>
```

5. 優先パスを確認します。

```
Get-SvmPreferredDataPath
```

プラグブル データベースのクローニング

プラグブル データベース (PDB) は、同じホストまたは代替ホスト上の別のターゲットCDBまたは同じターゲットCDBにクローニングできます。クローニングされたPDBを目的のSCNまたは日時にリカバリすることもできます。

始める前に

root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプト ディレクトリとポストスクリプト ディレクトリに手動で割り当てる必要があります。

手順

- 1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
- 2. [リソース] ページで、[表示] リストから [データベース] または [リソース グループ] を選択します。
- 3. データベースの詳細ビューまたはリソース グループの詳細ビューで、タイプが単一インスタンス（マルチテナント）のデータベースを選択します。

データベース トポロジのページが表示されます。

- 4. [Manage Copies]ビューで、ローカル コピー（プライマリ）、ミラー コピー（セカンダリ）、バックアップ コピー（セカンダリ）のいずれかのバックアップを選択します。
- 5. 表からバックアップを選択し、*をクリックします。 *。
- 6. [Name]ページで、次の操作を実行します。
 - a. *PDB クローン*を選択します。
 - b. クローニングするPDBを指定します。



PDBは一度に1つずつしかクローニングできません。

- c. クローンPDBの名前を指定します。
- 7. [Locations]ページで、次の操作を実行します。

フィールド	操作
Clone host	ソース データベース ホストがデフォルトで入力されています。 代替ホストにクローンを作成する場合は、ソース データベース ホストと同じバージョンのOracleおよびOSがインストールされているホストを選択します。
Target CDB	クローンPDBを含めるCDBを選択します。 ターゲットCDBが実行されていることを確認する必要があります。
Database State	PDB を READ-WRITE モードで開く場合は、クローンされた PDB を READ-WRITE モードで開く チェックボックスを選択します。

Datafile locations	データ ファイルの場所がデフォルトで入力されています。 SANファイルシステムまたはNFSファイルシステム用にSnapCenterで設定されているデフォルトの命名規則は、FileSystemNameofsourcedatabase_SCJOBIDです。 SnapCenterで設定されているASMディスク グループのデフォルトの命名規則は、SC_HASHCODEofDISKGROUP_SCJOBIDです。HASHCODEofDISKGROUPは、自動生成される2～10桁の数値で、各ASMディスク グループに固有です。  ASMディスク グループ名をカスタマイズする場合は、名前の長さがOracleでサポートされる最大長に準拠していることを確認してください。 別のパスを指定する場合は、クローン データベースのデータファイル マウント ポイントまたはASMディスク グループ名を入力する必要があります。

Oracleホーム、ユーザ名、およびグループの詳細が、ソース データベースから自動的に入力されます。値は、クローンが作成されるホストのOracle環境に基づいて変更できます。

8. [PreOps]ページで、次の手順を実行します。

- a. クローニング処理の前に実行するプリスクリプトのパスと引数を入力します。

プリスクリプトは、/var/opt/snapcenter/spl/scriptsまたはこのパス内の任意のフォルダに保存する必要があります。デフォルトでは、/var/opt/snapcenter/spl/scriptsがパスとして入力されています。スクリプトをこのパス内の任意のフォルダに配置した場合は、スクリプトの配置先となるフォルダまでの完全なパスを指定する必要があります。

SnapCenter、事前スクリプトと事後スクリプトを実行するときに、事前定義された環境変数を使用できます。"詳細情報"

- a. [Auxiliary CDB clone database parameter settings]セクションで、データベースの初期化に使用される事前入力されたデータベース パラメータの値を変更します。

9. *リセット*をクリックすると、デフォルトのデータベース パラメータ設定が取得されます。

10. PostOps ページでは、クローンされたデータベースのリカバリを実行するために、デフォルトで キャンセルまで が選択されます。

SnapCenter が適切なログ バックアップを見つけられない場合は、[キャンセルまで] オプションは選択されません。*外部アーカイブ ログの場所の指定*でログ バックアップが利用できない場合は、外部アーカイブ ログの場所を指定できます。ログの場所は複数指定できます。



フラッシュ リカバリ領域（FRA）とOracle Managed Files（OMF）をサポートするように設定されているソース データベースをクローニングする場合は、リカバリのログ デステーションもOMFディレクトリ構造に従っている必要があります。

フィールド名	説明
キャンセルまで	SnapCenterは、クローニング対象として選択されたデータ バックアップのあとに、破損していない一連のアーカイブ ログを含む最新のログ バックアップをマウントすることでリカバリを実行します。 プライマリ ストレージでクローニングを実行するには、ログとデータのバックアップをプライマリ ストレージに配置し、セカンダリ ストレージでクローニングを実行するには、ログとデータのバックアップをセカンダリ ストレージに配置する必要があります。クローン データベースは、欠落または破損したログ ファイルまでリカバリされます。
Date and time	SnapCenterは、指定された日時までデータベースをリカバリします。  時刻は24時間形式で指定できます。
Until SCN (System Change Number)	SnapCenterは、指定されたシステム変更番号（SCN） までデータベースをリカバリします。
Specify external archive log locations	外部アーカイブ ログの場所を指定します。
新しいDBIDを作成する	デフォルトでは、補助クローン データベースの 新しい DBID の作成 チェック ボックスは選択されていません。 ソース データベースと補助クローン データベースを区別するための一意の番号（DBID）を生成する場合は、このチェック ボックスを選択します。
一時表領域用の一時ファイルを作成する	クローン データベースのデフォルトの一時表領域用の一時ファイルを作成する場合は、このチェック ボックスを選択します。 このチェック ボックスをオフにすると、一時ファイルなしでデータベース クローンが作成されます。
Enter sql entries to apply when clone is created	クローンの作成時に適用するSQLエントリを追加します。

フィールド名	説明
Enter scripts to run after clone operation	クローニング処理のあとに実行するポストスクリプトのパスと引数を指定します。 ポストスクリプトは、<code>/var/opt/snapcenter/spl/scripts</code> またはこのパス内の任意のフォルダーに保存する必要があります。 デフォルトでは、<code>/var/opt/snapcenter/spl/scripts</code> パスが設定されます。スクリプトをこのパス内の任意のフォルダに配置した場合は、スクリプトの配置先となるフォルダまでの完全なパスを指定する必要があります。  クローニング処理が失敗した場合、ポストスクリプトは実行されず、クリーンアップ アクティビティが直接トリガーされます。

- 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。実行されたクローン操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

- 概要を確認し、[完了] をクリックします。
- モニター > ジョブ をクリックして、操作の進行状況を監視します。

終わったら

クローニングされたPDBのバックアップを作成する場合は、PDBのクローニング先となるターゲットCDBをバックアップする必要があります。クローニングされたPDBのみをバックアップすることはできません。セカンダリ関係を使用してバックアップを作成する場合は、ターゲットCDBのセカンダリ関係を作成する必要があります。

RACセットアップでは、クローニングされたPDBのストレージは、PDBのクローニングが実行されたノードにのみ接続されます。RACの他のノードのPDBはマウント状態です。クローニングされたPDBに他のノードからアクセスできるようにするには、ストレージを他のノードに手動で接続する必要があります。

詳細情報

- "ORA-00308 エラーメッセージが表示され、復元またはクローン作成が失敗する"
- "AIX システムでのバックアップ、復元、クローン操作のカスタマイズ可能なパラメータ"

UNIXコマンドを使用したOracleデータベース バックアップのクローニング

クローニング ワークフローには、計画、クローニング処理の実行、および処理の監視が含まれます。

このタスクについて

次に示すコマンドを実行して、Oracleデータベースのクローン仕様ファイルを作成し、クローニング処理を開始する必要があります。

コマンドで使用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンド リファレンス ガイド](#)"。

手順

1. 指定されたバックアップから Oracle データベース クローン仕様を作成します: *New-SmOracleCloneSpecification*



セカンダリ データ保護ポリシーが、統合されたmirror-vaultである場合は、`-IncludeSecondaryDetails`のみを指定します。`-SecondaryStorageType`を指定する必要はありません。

このコマンドによって、指定のソース データベースとそのバックアップに対して、Oracleデータベースのクローン仕様ファイルが自動的に作成されます。作成するクローン データベースに対して自動的に生成される値がこの仕様ファイルに取り込まれるようにするために、クローン データベースのSIDも指定する必要があります。



クローン仕様ファイルは、`/var/opt/snapcenter/sco/clone_specs` に作成されます。

2. クローン リソース グループまたは既存のバックアップからクローン操作を開始します: *New-SmClone*

このコマンドによってクローニング処理が開始されます。クローニング処理では、Oracleクローン仕様ファイルのパスを指定する必要もあります。リカバリ オプション、クローニング処理が実行されるホスト、プリスクリプト、ポストスクリプト、およびその他の詳細を指定することもできます。

デフォルトでは、クローン データベースのアーカイブ ログ保存先ファイルは、`$ORACLE_HOME/CLONE_SIDs` に自動的に設定されます。

Oracle Databaseクローンのスプリット

SnapCenterを使用して、クローン リソースを親リソースからスプリットできます。スプリットされたクローンは親リソースから独立します。

このタスクについて

- 中間クローンではクローン スプリット処理を実行できません。

たとえば、データベース バックアップからクローン1を作成したあとで、クローン1のバックアップを作成し、そのバックアップ（クローン2）をクローニングできます。クローン2を作成すると、クローン1は中間クローンになり、クローン1ではクローン スプリット処理を実行できなくなります。ただし、クロー

ン2に対してはクローン スプリット処理を実行できます。

クローン2をスプリットすると、クローン1は中間クローンではなくなるため、クローン1に対してクローン スプリット処理を実行できるようになります。

- クローンをスプリットすると、クローンのバックアップ コピーが削除されます。
- FlexCloneボリューム分割操作の詳細については、以下を参照してください。<https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["親ボリュームからのFlexCloneボリュームのスプリット"]
- ストレージ システム上のボリュームまたはアグリゲートがオンラインであることを確認します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] を選択します。
3. クローンされたリソース（データベースやLUNなど）を選択し、。
4. 分割するクローンの推定サイズとアグリゲート上で必要な空き容量を確認し、[開始] をクリックします。
5. モニター > ジョブ をクリックして、操作の進行状況を監視します。

SMCoreサービスが再起動し、クローン スプリット処理が実行されたデータベースが[Resources]ページにクローンとして表示されると、クローン スプリット処理が応答を停止します。Stop-SmJob コマンドレットを実行してクローン分割操作を停止し、クローン分割操作を再試行する必要があります。

クローンがスプリットされているかどうかを確認するためにポーリング時間を長く、または短くする必要がある場合は、SMCoreServiceHost.exe.configファイルのCloneSplitStatusCheckPollTimeパラメータの値を変更すると、SMCoreがクローン スプリット処理のステータスをポーリングする時間間隔を設定できます。値はミリ秒単位で、デフォルト値は5分です。

次に例を示します。

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```



バックアップ、リストア、または別のクローン スプリットが実行中の場合、クローン スプリットの開始処理は失敗します。クローン スプリット処理を再開するのは、実行中の処理が完了してからにしてください。

プラグブル データベースのクローンのスプリット

SnapCenterを使用して、プラグブル データベース（PDB）のクローンをスプリットできます。

このタスクについて

ターゲットCDBにPDBをクローニングし、ターゲットCDBのバックアップを作成した場合、PDBクローンをスプリットすると、クローニングされたPDBも、そのクローンPDBを含むターゲットCDBのすべてのバックアップから削除されます。



PDBクローンは、インベントリ ビューとリソース ビューのどちらにも表示されません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. リソース ビューまたはリソース グループ ビューからソース コンテナ データベース (CDB) を選択します。
3. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたは複製) ストレージ システムから クローン を選択します。
4. PDBクローン (targetCDB:PDBClone) を選択し、クリックします。 。
5. 分割するクローンの推定サイズとアグリゲート上で必要な空き容量を確認し、[開始] をクリックします。
6. モニター > ジョブ をクリックして、操作の進行状況を監視します。

Oracleデータベースのクローニング処理の監視

SnapCenterのクローニング処理の進捗状況を、[Jobs]ページで監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  てリストをフィルタリングし、クローニング処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*クローン*を選択します。
 - d. *ステータス*ドロップダウンリストからクローンのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. クローンジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

クローンの更新

Refresh-SmClone コマンドを実行してクローンを更新できます。このコマンドを実行すると、データベースのバックアップが作成され、既存のクローンは削除され、同じ名前のクローンが作成されます。



PDBクローンは更新できません。

必要なもの

- スケジュールされたバックアップを有効にしないで、オンライン フル バックアップまたはオフライン データ バックアップ ポリシーを作成します。
- ポリシーで、バックアップが失敗した場合に限り、Eメール通知を設定します。
- 不要なバックアップがなくなるように、オンデマンド バックアップの保持数を適切に定義します。
- クローン更新処理用に指定したリソース グループには、オンライン フル バックアップまたはオフライン データ バックアップ ポリシーのみが関連付けられていることを確認します。
- データベースが1つだけのリソース グループを作成します。
- クローン更新コマンド用にcronジョブを作成する場合は、データベース リソース グループでSnapCenter スケジュールとcronスケジュールが重なっていないことを確認します。

クローン更新コマンド用に作成したcronジョブでは、必ず24時間ごとにOpen-SmConnectionを実行します。

- クローンSIDがホストで一意であることを確認します。

複数のクローン更新処理で同じクローン仕様ファイルを使用する場合、または同じクローンSIDを指定してクローン仕様ファイルを使用する場合は、ホスト上でそのSIDを持つ既存のクローンは削除され、クローンは作成されます。

- バックアップ ポリシーがセカンダリ保護で有効になっていること、およびセカンダリ バックアップを使用してクローンを作成するために、クローン仕様ファイルが“-IncludeSecondaryDetails”を使用して作成されていることを確認します。
 - プライマリ クローン仕様ファイルが指定されているが、ポリシーでセカンダリ更新オプションが選択されている場合は、バックアップが作成され、更新がセカンダリに転送されます。ただし、クローンはプライマリ バックアップから作成されます。
 - プライマリ クローン仕様ファイルが指定され、ポリシーでセカンダリ更新オプションが選択されていない場合、バックアップはプライマリ上に作成され、クローンはプライマリから作成されます。

手順

1. 指定されたユーザーのSnapCenter Server との接続セッションを開始します: *Open-SmConnection*
2. 指定されたバックアップから Oracle データベース クローン仕様を作成します: *New-SmOracleCloneSpecification*



セカンダリ データ保護ポリシーが、統合されたmirror-vaultである場合は、
-IncludeSecondaryDetailsのみを指定します。-SecondaryStorageTypeを指定する必要はありません。

このコマンドによって、指定のソース データベースとそのバックアップに対して、Oracleデータベースのクローン仕様ファイルが自動的に作成されます。作成するクローン データベースに対して自動的に生成される値がこの仕様ファイルに取り込まれるようにするために、クローン データベースのSIDも指定する必要があります。



クローン仕様ファイルは、`/var/opt/snapcenter/sco/clone_specs` に作成されます。

3. `Refresh-SmClone` を実行します。

「PL-SCO-20032: canExecute 操作がエラーで失敗しました: PL-SCO-30031: Redo ログ ファイル +SC_2959770772_clmdb/clmdb/redolog/redo01_01.log が存在します」というエラー メッセージが表示されて操作が失敗する場合は、`-WaitToTriggerClone` に高い値を指定します。

UNIXコマンドの詳細については、"[SnapCenterソフトウェア コマンド リファレンス ガイド](#)"。

プラグブル データベースのクローンの削除

プラグブル データベース (PDB) のクローンが不要になった場合は削除できます。

ターゲットCDBにPDBがクローニングし、ターゲットCDBのバックアップを作成した場合、PDBクローンを削除すると、クローニングされたPDBもターゲットCDBのバックアップから削除されます。



PDBクローンは、インベントリ ビューとリソース ビューのどちらにも表示されません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. リソース ビューまたはリソース グループ ビューからソース コンテナ データベース (CDB) を選択します。
3. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたは複製) ストレージ システムからクローンを選択します。
4. PDBクローン (targetCDB:PDBClone) を選択し、クリックします。 。
5. [OK]をクリックします。

アプリケーション ボリュームの管理

アプリケーション ボリュームとは

アプリケーション ボリュームは、Oracleデータベースに関連する設定、インストーラ、その他データ以外のファイルなどの情報を格納するストレージです。

SnapCenter Plug-in for Oracle Databaseでは、アプリケーション ボリューム (データ ボリューム以外のボリ

ューム) およびOracleデータベースの整合性のあるバックアップを作成できます。

このプラグインによって、アプリケーション ボリュームのバックアップとクローニングが自動化されます。

- アプリケーション ボリュームとOracleデータベース ボリュームを1つのリソース グループ内で保護します。
- アプリケーション ボリュームのバックアップを作成します。
- アプリケーション ボリュームとともにOracleデータベースのバックアップを作成します。
- ポイントインタイムまでのアプリケーション ボリュームとともに、データベースのクローンを作成します。
- バックアップ処理のスケジュールを設定します。
- すべての処理を監視します。
- バックアップ処理とクローニング処理のレポートを表示します。

アプリケーション ボリュームの追加

SnapCenterは、Oracleデータベースのアプリケーション ボリュームのバックアップとクローニングをサポートしています。アプリケーション ボリュームは手動で追加する必要があります。アプリケーション ボリュームの自動検出はサポートされていません。



アプリケーション ボリュームでは、NFS直接接続とiSCSI直接接続のみがサポートされます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから Oracle データベース プラグインを選択します。
2. *アプリケーション ボリュームの追加*をクリックします。
3. [Name]ページで、次の操作を実行します。
 - [Name]フィールドにアプリケーション ボリュームの名前を入力します。
 - [Host Name]フィールドにホストの名前を入力します。
4. [Storage Footprint]ページで、ストレージ システム名を入力し、1つ以上のボリュームを選択し、関連付けられているLUNまたはqtreeを指定します。

複数のストレージ システムを追加できます。
5. 概要を確認し、[完了] をクリックします。
6. [リソース] ページで、[表示] リストから [アプリケーション ボリューム] を選択して、追加したすべてのアプリケーション ボリュームを表示します。

アプリケーション ボリュームの変更

バックアップが作成されていない場合は、アプリケーション ボリュームを追加したときに指定した値をすべて変更できます。バックアップが作成されている場合、変更できるのはストレージ システムの詳細のみです。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから Oracle データベース プラグインを選択します。
2. [リソース] ページで、[表示] リストから [アプリケーション ボリューム] を選択します。
3. クリック  値を変更します。
4. クリック  値を変更します。

アプリケーション ボリュームの削除

アプリケーション ボリュームに関連付けられているバックアップがある場合にアプリケーション ボリュームを削除すると、アプリケーション ボリュームはメンテナンス モードになり、新しいバックアップは作成されなくなり、以前のバックアップは保持されません。バックアップが関連付けられていない場合は、すべてのメタデータが削除されます。

必要に応じて、SnapCenterで削除操作を元に戻すことができます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから Oracle データベース プラグインを選択します。
2. [リソース] ページで、[表示] リストから [アプリケーション ボリューム] を選択します。
3. クリック  値を変更するには、[削除アイコン] をクリックします。

アプリケーション ボリュームのバックアップ

アプリケーション ボリュームのバックアップ

アプリケーション ボリュームがどのリソース グループにも含まれていない場合は、[Resources] ページからアプリケーション ボリュームをバックアップできます。

このタスクについて

デフォルトでは、整合グループ (CG) バックアップが作成されます。ボリュームベースのバックアップを作成する場合は、`web.config` ファイルで **EnableOracleNdvVolumeBasedBackup** の値を `true` に設定する必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから Oracle データベース プラグインを選択します。
2. [リソース] ページで、[表示] リストから [アプリケーション ボリューム] を選択します。
3. クリック *  *、ホスト名とデータベース タイプを選択してリソースをフィルターします。
をクリックします  フィルター パネルを閉じます。

4. バックアップするアプリケーション ボリュームを選択します。

[Application volume-Protect]ページが表示されます。

5. [Resource]ページで、次の操作を実行します。

フィールド	操作
Use custom name format for Snapshot copy	Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにしてから、名前形式を入力します。 たとえば、customtext__policy_hostname やresource_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。
Exclude archive log destinations from backup	バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。

6. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます 。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、  をクリックします。
- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリックします。

policy_name は、選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

7. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースに対して実行されたバックアップ操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

8. 概要を確認し、[完了] をクリックします。

アプリケーション ボリュームのトポロジ ページが表示されます。

9. *今すぐバックアップ*をクリックします。
10. [Backup]ページで次の手順を実行します。
 - a. リソースに複数のポリシーを適用している場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。
 - b. *バックアップ*をクリックします。
11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

アプリケーション ボリュームのリソース グループのバックアップ

アプリケーション ボリュームのみが含まれている、またはアプリケーション ボリュームとデータベースが混在しているリソース グループをバックアップできます。リソース グループのバックアップ処理は、リソース グループに定義されているすべてのリソースを対象に実行されます。

リソース グループに複数のアプリケーション ボリュームが含まれている場合は、すべてのアプリケーション ボリュームにSnapMirrorまたはSnapVaultのレプリケーション ポリシーを設定する必要があります。

このタスクについて

デフォルトでは、整合グループ (CG) バックアップが作成されます。ボリュームベースのバックアップを作成する場合は、`web.config` ファイルで **EnableOracleNdvVolumeBasedBackup** の値を `true` に設定する必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから Oracle データベース プラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。

リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、をクリックします。 *、タグを選択します。*をクリックします フィルター パネルを閉じます。

3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] をクリックします。
4. [Backup]ページで次の手順を実行します。
 - a. リソース グループに複数のポリシーを関連付けている場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*をクリックします。
5. モニター > ジョブ をクリックして、操作の進行状況を監視します。



検証処理はデータベースに対してのみ実行され、アプリケーション ボリュームに対しては実行されません。

アプリケーション ボリュームのバックアップのクローニング

SnapCenterを使用して、アプリケーション ボリュームのバックアップをクローニングできます。

始める前に

root以外のユーザとしてプラグインをインストールした場合は、実行権限をプリスクリプト ディレクトリとポストスクリプト ディレクトリに手動で割り当てる必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから Oracle データベース プラグインを選択します。
2. [リソース] ページで、[表示] リストから [アプリケーション ボリューム] を選択します。
3. アプリケーション ボリュームの詳細ビューまたはリソース グループの詳細ビューでアプリケーション ボリュームを選択します。

アプリケーション ボリュームのトポロジ ページが表示されます。

4. [Manage Copies]ビューで、ローカル コピー（プライマリ）、ミラー コピー（セカンダリ）、バックアップ コピー（セカンダリ）のいずれかのバックアップを選択します。
5. 表からバックアップを選択し、*をクリックします。  *。
6. [Location]ページで、次の操作を実行します。

フィールド	操作
プラグインホスト	クローンを作成するホストを選択します。
Target Resource Name	リソース名を指定します。

7. [Scripts]ページで、クローニング前に実行するスクリプトの名前、ファイルシステムをマウントするコマンド、およびクローニング後に実行するスクリプトの名前を指定します。
8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。実行されたクローン操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

9. 概要を確認し、[完了] をクリックします。

アプリケーション ボリュームのクローンのスプリット

SnapCenterを使用して、クローン リソースを親リソースからスプリットできます。スプリットされたクロー

ンは親リソースから独立します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから Oracle データベース プラグインを選択します。
2. [リソース] ページで、[表示] リストから [アプリケーション ボリューム] を選択します。
3. クローンしたリソースを選択してクリックします 。
4. 分割するクローンの推定サイズとアグリゲート上で必要な空き容量を確認し、[開始] をクリックします。
5. モニター > ジョブ をクリックして、操作の進行状況を監視します。

アプリケーション ボリュームのクローンの削除

不要と判断したクローンは削除することができます。他のクローンのソースのようにになっているクローンは削除できません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから Oracle データベース プラグインを選択します。
2. [リソース] ページで、[表示] リストから [アプリケーション ボリューム] を選択します。
3. リストからリソースまたはリソース グループを選択します。

リソースまたはリソース グループのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたは複製) ストレージ システムから クローン を選択します。
5. クローンを選択し、 をクリックします。
6. [Delete Clone] ページで、次の操作を実行します。
 - a. クローン削除前 フィールドに、クローンを削除する前に実行するスクリプトの名前を入力します。
 - b. アンマウント フィールドに、クローンを削除する前にクローンをアンマウントするコマンドを入力します。
7. [OK] をクリックします。

Windows ファイルシステムの保護

SnapCenter Plug-in for Microsoft Windows の概念

SnapCenter Plug-in for Microsoft Windows の概要

SnapCenter Plug-in for Microsoft Windows は、Microsoft ファイルシステムのリソースに対応したデータ保護管理を提供する、NetApp SnapCenter ソフトウェアのホスト側コンポーネントです。Windows ファイルシステムのストレージのプロビジョニング、整合性のある Snapshot の作成、およびスペースの再生が可能です。Plug-in for Windows を使用することで、SnapCenter 環境でのファイルシステムのバックアップ、リストア、およびクローニングの処理を自動化できます。

Plug-in for Windows がインストールされている場合は、SnapCenter で NetApp SnapMirror テクノロジーを使用して別のボリュームにバックアップ セットのミラー コピーを作成できるほか、NetApp SnapVault テクノロジーを使用してアーカイブや標準への準拠を目的としたディスクツーディスク バックアップ レプリケーションを実行できます。

- SnapCenter 環境の Windows ホストで実行されている他のプラグインに対してアプリケーション対応のデータ保護が有効になります。
- SnapCenter 環境の Microsoft ファイルシステムに対するアプリケーション対応のバックアップ、リストア、クローニングの各処理が自動化されます。
- Windows ホストのストレージ プロビジョニング、整合性のある Snapshot の作成、およびスペース再生がサポートされます。



Plug-in for Windows では、物理 LUN と RDM LUN で SMB 共有および Windows ファイルシステムをプロビジョニングできますが、SMB 共有での Windows ファイルシステムのバックアップ処理はサポートされません。

SnapCenter Plug-in for Microsoft Windows の機能

Plug-in for Windows をインストールした環境では、SnapCenter を使用して Windows ファイルシステムをバックアップ、リストア、およびクローニングすることができます。これらの処理をサポートするタスクも実行できます。

- リソースの検出
- Windows ファイルシステムのバックアップ
- バックアップ処理のスケジュールの設定
- ファイルシステムのバックアップのリストア
- ファイルシステムのバックアップのクローニング
- バックアップ、リストア、クローニングの各処理を監視する



Plug-in for Windows では、SMB 共有のファイルシステムのバックアップとリストアはサポートされていません。

SnapCenter Plug-in for Windowsの特長

Plug-in for Windowsは、ストレージ システム上でNetAppのSnapshotテクノロジーと統合されます。Plug-in for Windowsの操作には、SnapCenterのインターフェイスを使用します。

Plug-in for Windowsの主な機能は次のとおりです。

- * SnapCenterによる統合グラフィカル ユーザー インターフェイス*

SnapCenterのインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。どのプラグインでも、SnapCenterのインターフェイスから、バックアップ プロセスとリストア プロセスを一貫した方法で実行できるほか、ダッシュボード ビューで概要を把握したり、ロールベース アクセス制御（RBAC）を設定したり、ジョブを監視したりすることができます。また、SnapCenterでは、バックアップとクローニングの処理に対応したスケジュールとポリシーの一元管理もサポートされます。

- 自動化された中央管理

日常的なファイルシステムのバックアップのスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理をセットアップしたりできます。SnapCenterからのEメール アラートの送信を設定して、ファイルシステム環境をプロアクティブに監視することもできます。

- 無停止の**NetApp**スナップショットテクノロジー

Plug-in for Windowsでは、NetAppのSnapshotテクノロジーを使用しています。これにより、ファイルシステムを数秒でバックアップし、ホストをオフラインにすることなく迅速にリストアすることが可能です。Snapshotはストレージ スペースを最小限しか消費しません。

Plug-in for Windowsには、上記の主要な機能以外にも次のようなメリットがあります。

- バックアップ、リストア、およびクローニングのワークフローがサポートされます。
- セキュリティがRBACでサポートされ、ロール委譲が一元化されます。
- NetApp FlexCloneテクノロジーを使用して、テストまたはデータ抽出に使用する本番環境ファイルシステムのコピー（スペース効率に優れたコピー）を作成できます。

FlexCloneのライセンス情報については、以下を参照してください。["SnapCenterのライセンス"](#)。

- 複数のサーバで同時に複数のバックアップを実行できます。
- PowerShellコマンドレットを使用してバックアップ、リストア、およびクローニングの処理のスクリプトを作成できます。
- ファイルシステムと仮想マシン ディスク（VMDK）のバックアップがサポートされます。
- 物理インフラと仮想インフラがサポートされます。
- iSCSI、ファイバチャネル、FCoE、rawデバイス マッピング（RDM）、非対称LUNマッピング（ALM）、NFSおよびVMFS経由のVMDK、および仮想FCがサポートされます。
- Windows Server 2022でNon-Volatile Memory express（NVMe）がサポートされます。
 - NVMe over TCP/IPで作成されたVMDKレイアウト上のバックアップ、リストア、クローニング、検証の各ワークフロー。

- ESX 8.0 Update 2以降のNVMeファームウェア バージョン1.3をサポートします。仮想マシン ハードウェア バージョン21が必要です。
- Windows Serverフェイルオーバー クラスタリング (WSFC) は、NVMe over TCP/IP上のVMDKを介したアプリケーションではサポートされません。
- サイト全体の障害時でもビジネス サービスの運用を継続できるようにするSnapMirrorアクティブ シンク (当初はSnapMirror Business Continuity [SM-BC] としてリリース) をサポートし、セカンダリ コピーを使用してアプリケーションを透過的にフェイルオーバーできるようにします。SnapMirrorアクティブ同期でフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。

SnapCenterでのWindowsファイルシステムのバックアップ方法

SnapCenterでは、Snapshotテクノロジーを使用してWindowsファイルシステムのリソースがバックアップされます。これには、WindowsクラスタのLUN、CSV（クラスタ共有ボリューム）、RDM（rawデバイス マッピング）ボリューム、ALM（非対称LUNマッピング）、およびVMFS / NFS（NFSを使用するVMware Virtual Machine File System）に基づくVMDKにあるリソースが含まれます。

SnapCenterでは、ファイルシステムのSnapshotを作成することによってバックアップを作成します。ボリュームに複数のホストのLUNが含まれている場合は、フェデレーテッド バックアップを使用すると、各LUNを個別にバックアップするよりも迅速かつ効率的に処理できます。ボリュームのSnapshotを1つだけ作成すれば、各ファイルシステムのSnapshotを個別に作成しなくても済むからです。

SnapCenterで作成されるSnapshotには、ストレージ システム ボリューム全体がキャプチャされます。ただし、このバックアップは、バックアップが作成されたホスト サーバに対してのみ有効になります。

他のホスト サーバのデータが同じボリュームに含まれている場合、それらのデータをSnapshotからリストアすることはできません。



Windowsファイルシステムにデータベースが含まれている場合、ファイルシステムをバックアップしてもデータベースがバックアップされるわけではありません。データベースをバックアップするには、いずれかのデータベース用プラグインを使用する必要があります。

SnapCenter Plug-in for Microsoft Windowsでサポートされるストレージ タイプ

SnapCenterは、物理マシンと仮想マシンの両方でさまざまなストレージ タイプをサポートしています。ホストに対応したパッケージをインストールする前に、ストレージ タイプがサポートされているかどうかを確認する必要があります。

Windows Serverでは、SnapCenterによるプロビジョニングとデータ保護がサポートされます。サポートされているバージョンに関する最新情報について

は、[https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT\[\"NetApp Interoperability Matrix Tool\"\]](https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT[\)。

マシン	ストレージ タイプ	プロビジョニングを使用して	サポートノート
物理サーバ	FC接続LUN	SnapCenterのグラフィカル ユーザ インターフェイス (GUI) またはPowerShellコマンドレット	
物理サーバ	iSCSI接続LUN	SnapCenterのGUIまたはPowerShellコマンドレット	
物理サーバ	Storage Virtual Machine (SVM) 上のSMB3 (CIFS) 共有	SnapCenterのGUIまたはPowerShellコマンドレット	プロビジョニングのみがサポートされます。
VMware VM	FCまたはiSCSI HBAで接続されたRDM LUN	PowerShellコマンドレット	
VMware VM	iSCSIイニシエータでゲスト システムに直接接続されたiSCSI LUN	SnapCenterのGUIまたはPowerShellコマンドレット	
VMware VM	仮想マシン ファイルシステム (VMFS) またはNFSデータストア	VMware vSphere	
VMware VM	SVM上のSMB3共有に接続されたゲスト システム	SnapCenterのGUIまたはPowerShellコマンドレット	プロビジョニングのみがサポートされます。
VMware VM	NFSとSANの両方に存在するvVolデータストア	ONTAP Tools for VMware vSphere	

マシン	ストレージ タイプ	プロビジョニングを使用して	サポートノート
Hyper-V VM	仮想ファイバチャネル スイッチで接続された仮想FC (vFC) LUN	SnapCenterのGUIまたはPowerShellコマンドレット	仮想ファイバチャネル スイッチで接続された仮想FC (vFC) LUNのプロビジョニングには、Hyper-V Managerを使用する必要があります。  Hyper-Vのパススルーディスク、およびNetAppストレージでプロビジョニングされたVHD (VHDX) でのデータベースのバックアップはサポートされません。
Hyper-V VM	iSCSIイニシエータでゲスト システムに直接接続されたiSCSI LUN	SnapCenterのGUIまたはPowerShellコマンドレット	 Hyper-Vのパススルーディスク、およびNetAppストレージでプロビジョニングされたVHD (VHDX) でのデータベースのバックアップはサポートされません。

マシン	ストレージ タイプ	プロビジョニングを使用して	サポートノート
Hyper-V VM	SVM上のSMB3共有に接続されたゲスト システム	SnapCenterのGUIまたはPowerShellコマンドレット	プロビジョニングのみがサポートされます。  Hyper-Vのパススルーディスク、およびNetAppストレージでプロビジョニングされたVHD (VHDX) でのデータベースのバックアップはサポートされません。

Windows プラグインに必要な最小ONTAP権限

必要な最小ONTAP権限は、データ保護に使用するSnapCenterプラグインによって異なります。

- 全アクセス コマンド: ONTAP 9.12.1 以降に必要な最小限の権限

- event generate-autosupport-log
- job history show
- job stop
- lun
- lun create
- lun delete
- lun igroup add
- lun igroup create
- lun igroup delete
- lun igroup rename
- lun igroup show
- lun mapping add-reporting-nodes
- lun mapping create
- lun mapping delete
- lun mapping remove-reporting-nodes

- lun mapping show
- lun modify
- lun move-in-volume
- lun offline
- lun online
- lun resize
- lun serial
- lun show
- snapmirror policy add-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- snapmirror restore
- snapmirror show
- snapmirror show-history
- snapmirror update
- snapmirror update-ls-set
- snapmirror list-destinations
- version
- volume clone create
- volume clone show
- volume clone split start
- volume clone split stop
- volume create
- volume destroy
- volume file clone create
- volume file show-disk-usage
- volume offline
- volume online
- volume modify
- volume qtree create
- volume qtree delete
- volume qtree modify
- volume qtree show
- volume restrict
- volume show
- volume snapshot create

- volume snapshot delete
- volume snapshot modify
- volume snapshot rename
- volume snapshot restore
- volume snapshot restore-file
- volume snapshot show
- volume unmount
- vserver cifs
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy show
- vserver cifs share show
- vserver cifs show
- vserver export-policy
- vserver export-policy create
- vserver export-policy delete
- vserver export-policy rule create
- vserver export-policy rule show
- vserver export-policy show
- vserver iscsi
- vserver iscsi connection show
- vserver show
- 読み取り専用コマンド: ONTAP 8.3.0以降に必要な最小限の権限
 - ネットワークインターフェース
 - network interface show
 - SVM

SnapMirrorレプリケーションと**SnapVault**レプリケーションのためのストレージ システムの準備

SnapCenterプラグインと一緒にONTAP SnapMirrorテクノロジーを使用すると、バックアップセットのミラー コピーを別のボリュームに作成できます。また、ONTAP SnapVaultを使用すれば、標準への準拠やその他のガバナンスを目的としたディスクツリー ディスクのバックアップ レプリケーションを実行できます。これらのタスクを実行する前に、ソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenterは、Snapshot処理の完了後に、SnapMirrorとSnapVaultに対する更新を実行します。SnapMirror更新とSnapVault更新は、SnapCenterジョブの一部として実行されるため、ONTAPスケジュールを別途作成しないでください。



NetApp SnapManager製品からSnapCenterに移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリ ストレージ（ソース ボリューム）上のデータがセカンダリ ストレージ（デスティネーション ボリューム）にレプリケートされます。この関係を初期化すると、ソース ボリュームで参照されるデータ ブロックがデスティネーション ボリュームに転送されます。



SnapCenter は、SnapMirrorとSnapVaultボリューム間のカスケード関係をサポートしていません（* プライマリ * > ミラー > ボールト）。ファンアウト関係を使用する必要があります。

SnapCenterは、バージョンに依存しないSnapMirror関係の管理をサポートしています。バージョンに依存しないSnapMirror関係とその設定方法の詳細については、["ONTAPのドキュメント"](#)。

Windows ファイルシステムのバックアップ戦略の定義

バックアップを作成する前にバックアップ戦略を定義しておく、ファイルシステムの正常なリストアやクローニングに必要なバックアップを作成できます。バックアップ戦略の大部分は、サービス レベル アグリーメント（SLA）、目標復旧時間（RTO）、および目標復旧時点（RPO）によって決まります。

SLAとは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。RTOは、サービスの停止からビジネス プロセスの復旧までに必要となる時間です。RPOは、障害発生後に通常処理を再開するためにバックアップ ストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA、RTO、およびRPOは、データ保護戦略に関与します。

Windows ファイルシステムのバックアップ スケジュール

バックアップ頻度はポリシーで指定され、バックアップ スケジュールはリソース グループの設定で指定されます。バックアップの頻度またはスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更新率とデータの重要性です。使用頻度の高いリソースは1時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは1日に1回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービス レベル アグリーメント（SLA）、目標復旧時点（RPO）などがあります。

SLAは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。RPOは、障害発生後に通常処理を再開するためにバックアップ ストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLAとRPOはデータ保護戦略に関わる要件です。

使用頻度の高いリソースであっても、フル バックアップは1日に1～2回で十分です。

バックアップ スケジュールには、次の2つの要素があります。

- バックアップ頻度

バックアップ頻度 (バックアップを実行する頻度) は、一部のプラグインでは スケジュール タイプ と呼ばれ、ポリシー構成の一部です。たとえば、バックアップ頻度を時間ごと、日ごと、週ごと、または月ごとに設定することも、ポリシーをオンデマンドのみのポリシーにする「なし」を指定することもできます。設定 > ポリシー をクリックすると、ポリシーにアクセスできます。

- バックアップ スケジュール

バックアップ スケジュール（バックアップが実行される日時）は、リソース グループ設定の一部です。たとえば、週次バックアップのポリシーが構成されたリソース グループがある場合は、毎週木曜日の午後 10 時にバックアップするようにスケジュールを構成できます。リソース > リソース グループ をクリックすると、リソース グループのスケジュールにアクセスできます。

Windows ファイルシステムで必要なバックアップの数

必要なバックアップの数を左右する要因としては、Windows ファイルシステムのサイズ、使用中のボリュームの数、ファイルシステムの変更率、サービス レベル アグリーメント（SLA）などがあります。

Windows ファイルシステムのバックアップ命名規則

Windows ファイルシステムのバックアップでは、Snapshot のデフォルトの命名規則が使用されます。デフォルトのバックアップ命名規則では Snapshot 名にタイムスタンプが追加されるので、コピーが作成されたタイミングを特定できます。

Snapshot では、次のデフォルトの命名規則が使用されます。resourcegroupname_hostname_timestamp

バックアップ リソース グループには、次の例のように論理的な名前を付ける必要があります。

```
dtst1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- `dtst1` リソース グループ名です。
- `mach1x88` ホスト名です。
- `03-12-2015\_23.17.26` 日付とタイムスタンプです。

バックアップの作成時に、バックアップを識別するためのタグを追加することもできます。一方、カスタマイズしたバックアップ命名規則を使用する場合は、バックアップ処理の完了後にバックアップの名前を変更する必要があります。

バックアップ保持オプション

バックアップ コピーを保持する日数を選択するか、または保持するバックアップ コピーの数（ONTAP では最大 255 個のコピー）を指定することができます。たとえば、組織の必要に応じて、10 日分のバックアップ コピーや 130 個のバックアップ コピーを保持できます。

ポリシーを作成する際に、バックアップ タイプおよびスケジュール タイプの保持オプションを指定できます。

SnapMirror レプリケーションを設定すると、デスティネーション ボリュームに保持ポリシーがミラーリングされます。

SnapCenter は、スケジュール タイプに一致する保持ラベルを持つ保持されたバックアップを削除します。リソースまたはリソース グループに対してスケジュール タイプが変更されると、古いスケジュール タイプ ラベルのバックアップがシステムに残ることがあります。



バックアップ コピーを長期にわたって保持する場合は、SnapVault/バックアップを使用する必要があります。

Windows ファイルシステムのクローンのソースとデスティネーション

ファイルシステムのクローニングは、プライマリ ストレージから行うこともセカンダリ ストレージから行うこともできます。デスティネーションについても、要件に応じて、バックアップの元の場所のほか、同じホストまたは別のホストの別の場所を選択することが可能です。クローンのデスティネーションのボリュームは、ソースのバックアップと同じである必要があります。

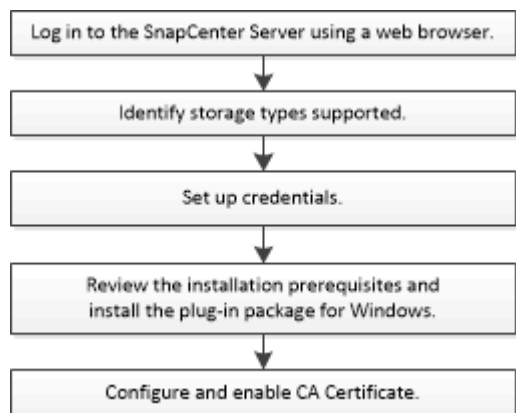
クローン先	説明
元のソースの場所	SnapCenterでは、デフォルトでは、クローニングされたバックアップと同じホストの同じ場所にクローンが格納されます。
別の場所	同じホストまたは別のホストの別の場所にクローンを格納できます。ホストでStorage Virtual Machine (SVM) への接続が設定されている必要があります。

クローニング処理の完了後にクローンの名前を変更することができます。

SnapCenter Plug-in for Microsoft Windowsのインストール

SnapCenter Plug-in for Microsoft Windowsのインストール ワークフロー

データベース ファイルではない Windows ファイルを保護する場合は、Microsoft Windows 用のSnapCenterプラグインをインストールして設定する必要があります。



SnapCenter Plug-in for Microsoft Windowsのインストール要件

Plug-in for Windowsをインストールする前に、特定のインストール要件を確認しておく必要があります。

ユーザがPlug-in for Windowsの使用を開始するためには、SnapCenter管理者が事前にSnapCenter Serverをインストールして設定し、前提条件となるタスクを実行する必要があります。

- Plug-in for Windowsをインストールするには、SnapCenter admin権限が必要です。

SnapCenter adminロールには管理者権限が必要です。

- SnapCenter Serverをインストールして設定しておく必要があります。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。
- バックアップ レプリケーションが必要な場合は、SnapMirrorとSnapVaultをセットアップする必要があります。

SnapCenter Plug-ins Package for Windowsをインストールするホストの要件

SnapCenter Plug-ins Package for Windowsをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	Microsoft Windows サポートされているバージョンに関する最新情報については、" NetApp Interoperability Matrix Tool "。 Windows クラスター セットアップを使用している場合は、Windows リモート管理 (WinRM) もインストールして構成する必要があります。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	5 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell Core 7.4.2 サポートされているバージョンに関する最新情報については、" NetApp Interoperability Matrix Tool "。

Plug-in for Windowsのクレデンシャルの設定

SnapCenterは、クレデンシャルを使用してSnapCenterの処理を実行するユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、Windowsファイルシステムでのデータ保護処理に使用するクレデンシャルをそれぞれ作成する必要があります。

必要なもの

- プラグインのインストール前にWindowsクレデンシャルを設定する必要があります。
- このクレデンシャルには、管理者権限（リモート ホストに対する管理者権限を含む）を設定する必要があります。
- 個々のリソース グループのクレデンシャルを設定する場合で、ユーザに完全なadmin権限が割り当てられていない場合は、少なくともリソース グループとバックアップの権限を割り当てる必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[資格情報]をクリックします。
3. *新規*をクリックします。
4. [Credential]ページで次の操作を実行します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。

フィールド	操作
ユーザー名/パスワード	認証に使用するユーザ名とパスワードを入力します。 - ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者またはSnapCenterプラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。ユーザ名フィールドの有効な形式は次のとおりです。 - NetBIOS\UserName - Domain FQDN\UserName - UserName@upn - ローカル管理者（ワークグループの場合のみ） ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。ユーザー名フィールドの有効な形式は次のとおりです。 UserName パスワードには二重引用符 (") やバッククォート (') を使用しないでください。未満記号 (<) と感嘆符 (!) を組み合わせて使用したりしないでください。たとえば、lessthan<!10、lessthan10<!、バックティック `12 などです。
パスワード	認証に使用するパスワードを入力します。

5. [OK]をクリックします。

クレデンシャルの設定が完了したら、必要に応じて[User and Access]ページでユーザやユーザ グループにクレデンシャルを割り当てることができます。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、作成したグループ管理サービス アカウント（gMSA）を通じて、管理対象ドメイン アカウントからサービス アカウントのパスワードを自動管理できます。

開始する前に

- Windows Server 2016以降のドメイン コントローラが必要です。
- ドメインのメンバーであるWindows Server 2016以降のホストが必要です。

手順

1. KDSルート キーを作成し、gMSA内のオブジェクトごとに一意のパスワードを生成します。
2. 各ドメインについて、Windowsドメインコントローラから次のコマンドを実行します: Add-KDSRootKey -EffectiveImmediately
3. gMSAを作成して設定します。
 - a. 次の形式でユーザ グループ アカウントを作成します。

```
domainName\accountName$  
.. コンピュータ オブジェクトをグループに追加します。  
.. 作成したユーザ グループを使用してgMSAを作成します。
```

次に例を示します。

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 走る `Get-ADServiceAccount` サービス アカウントを確認するコマンド。
```

4. ホストでgMSAを設定します。
 - a. gMSAアカウントを使用するホストで、Windows PowerShell用のActive Directoryモジュールを有効にします。

これを行うには、PowerShellから次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. ホストを再起動します。
- b. PowerShell コマンド プロンプトから次のコマンドを実行して、ホストに gMSA をインストールします。 `Install-AdServiceAccount <gMSA>`
- c. 次のコマンドを実行して、gMSA アカウントを確認します。 `Test-AdServiceAccount <gMSA>`
5. ホスト上の設定済みgMSAに管理者権限を割り当てます。
6. SnapCenter Serverで設定済みのgMSAアカウントを指定してWindowsホストを追加します。

SnapCenter Serverにより、選択したプラグインがホストにインストールされ、プラグインのインストール時には指定したgMSAがサービスのログオン アカウントとして使用されます。

ホストの追加とSnapCenter Plug-in for Microsoft Windowsのインストール

SnapCenterの[Add Host]ページを使用して、Windowsホストを追加できます。SnapCenter Plug-in for Microsoft Windowsは、指定したホストに自動的にインストールされます。これは推奨されるプラグインのインストール方法です。ホストの追加とプラグインのインストールは、ホストごとまたはクラスタごとに実行できます。

開始する前に

- SnapCenter Serverホストのオペレーティング システムがWindows 2019で、プラグイン ホストのオペレーティング システムがWindows 2022の場合は、次の手順を実行する必要があります。
 - Windows Server 2019 (OSビルド17763.5936) 以降にアップグレードする
 - Windows Server 2022 (OSビルド20348.2402) 以降にアップグレードする
- この処理は、SnapCenter Adminロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。

- SnapCenterユーザーを、Windows Server の「サービスとしてログオン」 ロールに追加する必要があります。
- メッセージ キュー サービスが実行中であることを確認する必要があります。
- グループ管理サービス アカウント（gMSA）を使用する場合は、管理者権限でgMSAを設定する必要があります。

"Windows Server 2016以降でWindowsファイルシステム用にグループ管理サービス アカウントを設定する"

タスク概要

- SnapCenter Serverをプラグイン ホストとして別のSnapCenter Serverに追加することはできません。
- Windowsプラグイン
 - Microsoft Windows
 - Microsoft Exchange Server
 - Microsoft SQL Server
 - SAP HANA

- クラスタへのプラグインのインストール

クラスタ（WSFC、Oracle RAC、またはExchange DAG）にプラグインをインストールする場合、プラグインはクラスタのすべてのノードにインストールされます。

- Eシリーズ ストレージ

Eシリーズ ストレージに接続されたWindowsホストにPlug-in for Windowsをインストールすることはできません。



SnapCenterでは、同じホスト（プラグイン ホスト）をSnapCenterに追加することはできません。そのホストがすでにワークグループに属していて、ドメインを別のものに変更しても（またはその逆をしても）、追加することはできません。同じホストを追加する場合は、SnapCenterからホストを削除して再度追加する必要があります。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. 上部で*管理対象ホスト*が選択されていることを確認します。
3. *[追加]*をクリックします。
4. [Hosts]ページで次の操作を実行します。

フィールド	操作
ホストタイプ	Windows タイプのホストを選択します。 SnapCenter Serverがホストを追加し、Plug-in for Windowsをホストにインストールします（プラグインがまだインストールされていない場合）。

フィールド	操作
ホスト名	ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。 SnapCenterが機能するためには、DNSが適切に設定されている必要があります。したがって、ベストプラクティスはFQDNを入力することです。 次のいずれかのIPアドレスまたはFQDNを入力できます。 • スタンドアロン ホスト • Windows Serverフェイルオーバー クラスタリング（WSFC） SnapCenterを使用してホストを追加する際、ホストがサブドメインの一部である場合は、FQDNを指定する必要があります。
Credentials	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモート ホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 ユーザ名、ドメイン、およびホスト タイプを含むクレデンシャルの詳細は、指定したクレデンシャルの名前にカーソルを合わせると表示されます。  認証モードは、[Add Host]ウィザードで指定するホスト タイプによって決まります。

5. [Select Plug-ins to Install]セクションで、インストールするプラグインを選択します。

新規導入の場合、プラグイン パッケージは表示されません。

6. (オプション) [その他のオプション] をクリックします。

フィールド	操作
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。 デフォルトのポート番号は8145です。SnapCenter Serverがカスタム ポートにインストールされている場合は、そのポート番号がデフォルト ポートとして表示されます。  プラグインを手動でインストールしてカスタム ポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理が失敗します。
Installation Path	デフォルトのパスはC:\Program Files\NetApp\SnapCenterです。 必要に応じて変更できます。SnapCenter Plug-ins Package for Windowsの場合、デフォルト パスはC:\Program Files\NetApp\SnapCenterです。ただし、必要に応じて、デフォルト パスはカスタマイズできます。
クラスター内のすべてのホストを追加する	WSFC内のすべてのクラスター ノードを追加するには、このチェック ボックスをオンにします。
Skip preinstall checks	プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェック ボックスをオンにします。
Use group Managed Service Account (gMSA) to run the plug-in services	グループ管理サービス アカウント (gMSA) を使用してプラグイン サービスを実行する場合は、このチェック ボックスをオンにします。 gMSA 名を次の形式で指定します: domainName\accountName\$。  gMSAは、SnapCenter Plug-in for Windowsサービスのログオン サービス アカウントとしてのみ使用されます。

7. *送信*をクリックします。

「事前チェックをスキップ」チェックボックスを選択していない場合、ホストがプラグインのインストール要件を満たしているかどうかを検証されます。ディスク容量、RAM、PowerShellのバージョン、.NETのバージョン、および場所が最小要件に照らして検証されます。最小要件を満たしていない場合、対応す

るエラーまたは警告メッセージが表示されます。

エラーがディスク容量またはRAMに関連している場合は、次の場所にあるweb.configファイルを更新できます。`C:\Program Files\NetApp\SnapCenter` デフォルト値を変更する WebApp。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。



HAのセットアップでweb.configファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. インストールの進捗状況を監視します。

PowerShellコマンドレットを使用した複数のリモート ホストへのSnapCenter Plug-in for Microsoft Windowsのインストール

SnapCenter Plug-in for Microsoft Windowsを複数のホストに一度にインストールする場合は、`Install-SmHostPackage` PowerShell コマンドレット。

プラグインをインストールする各ホストで、ローカル管理者の権限を持つドメイン ユーザとしてSnapCenterにログインしている必要があります。

手順

1. PowerShellを起動します。
2. SnapCenter Serverホストで、`Open-SmConnection`コマンドレットを実行し、資格情報を入力します。
3. スタンドアロンホストまたはクラスタをSnapCenterに追加するには、`Add-SmHost`コマンドレットと必要なパラメータ。

コマンドレットで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

4. 複数のホストにプラグインをインストールするには、`Install-SmHostPackage`コマンドレットと必要なパラメータ。

使用することができます`-skipprecheck`プラグインを手動でインストールし、ホストがプラグインのインストール要件を満たしているかどうかを検証したくない場合は、このオプションを選択します。

コマンドラインからのSnapCenter Plug-in for Microsoft Windowsのサイレント インストール

SnapCenter GUIからリモートでインストールできない場合は、Windowsホスト上でローカルにSnapCenter Plug-in for Microsoft Windowsをインストールできます。Windowsのコマンドラインから、SnapCenter Plug-in for Microsoft Windowsのインストール プログラムをサイレント モードで自動的に実行できます。

開始する前に

- ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドルがインストールされている必要があります。
- PowerShell 7.4.2以降がインストールされている必要があります。

- ホストのローカル管理者である必要があります。

手順

1. インストールの場所から、SnapCenter Plug-in for Microsoft Windowsをダウンロードします。

たとえば、デフォルトのインストール パスはC:\ProgramData\NetApp\SnapCenter\Package Repositoryです。

このパスには、SnapCenter Serverがインストールされているホストからアクセスできます。

2. プラグインをインストールするホストにインストール ファイルをコピーします。
3. コマンド プロンプトから、インストール ファイルをダウンロードしたディレクトリに移動します。
4. 以下のコマンドを、変数を実際のデータに置き換えて入力します。

```
"snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
ISFeatureInstall=SCW
```

例えば：

```
`"C:\ProgramData\NetApp\SnapCenter\Package Repository
\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:
\HPPW_SCW_Install.log" /log"C:\ BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password
ISFeatureInstall=SCW`
```



Plug-in for Windowsのインストール時に渡されるすべてのパラメータでは、大文字と小文字が区別されます。

以下の変数に値を入力します。

変数	Value
/debuglog"<デバッグログパス>	次の例のように、スイート インストーラー ログ ファイルの名前と場所を指定します: Setup.exe /debuglog"C:\PathToLog\setupexe.log"。
BI_SNAPCENTER_PORT	SnapCenterがSMCoreと通信するポートを指定します。
SUITE_INSTALLDIR	ホストのプラグイン パッケージのインストール ディレクトリを指定します。
BI_SERVICEACCOUNT	SnapCenter Plug-in for Microsoft WindowsのWebサービス アカウントを指定します。

変数	Value
BI_SERVICEPWD	SnapCenter Plug-in for Microsoft WindowsのWebサービス アカウントのパスワードを指定します。
ISFeatureInstall	SnapCenterでリモート ホストに導入するソリューションを指定します。

debuglog パラメータには、SnapCenterのログ ファイルのパスが含まれます。このログ ファイルにはインストールで実行されるプラグインの前提条件に関するチェック結果が記録されるため、トラブルシューティング情報を入手する手段としてこのログ ファイルに書き込むことを推奨します。

必要な場合、SnapCenter for Windowsパッケージのログ ファイルでその他のトラブルシューティング情報を確認できます。パッケージのログ ファイルは、*%Temp%* フォルダー (例: *C:\temp*) に (古いものから順に) リストされます。



Plug-in for Windowsをインストールすると、SnapCenter Serverではなくホストにプラグインが登録されます。SnapCenter GUIまたはPowerShellコマンドレットを使用してホストを追加することにより、SnapCenter Serverにプラグインを登録できます。ホストを追加すると、プラグインが自動的に検出されます。

SnapCenterプラグイン パッケージのインストール ステータスの監視

[Jobs]ページを使用して、SnapCenterプラグイン パッケージのインストールの進捗状況を監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、プラグインのインストール操作のみがリストされるようにリストをフィルタリングするには、次の手順を実行します。
 - a. *フィルター*をクリックします。
 - b. オプション：開始日と終了日を指定します。

- c. [タイプ] ドロップダウン メニューから、[プラグインのインストール] を選択します。
 - d. [Status] ドロップダウン メニューから、インストールのステータスを選択します。
 - e. *適用*をクリックします。
4. インストール ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
 5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

CA証明書の設定

CA証明書CSRファイルの生成

証明書署名要求（CSR）を生成し、生成したCSRを使用して認証局（CA）から取得した証明書をインポートできます。証明書には秘密キーが関連付けられます。

CSRはエンコードされたテキストのブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。



CA 証明書の RSA キーの長さは最低 3072 ビットである必要があります。

CSRを生成するための情報については、["CA証明書CSRファイルの生成方法"](#)。



ドメイン (*.domain.company.com) またはシステム (machine1.domain.company.com) の CA 証明書を所有している場合は、CA 証明書 CSR ファイルの生成をスキップできます。SnapCenterを使用して、既存のCA証明書を導入できます。

クラスタ構成の場合、クラスタ名（仮想クラスタFQDN）と、それぞれのホスト名がCA証明書に記載されている必要があります。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。ワイルドカード証明書 (*.domain.company.com) の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenter ServerとWindowsホスト プラグインにCA証明書をインポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
4. コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書 をクリックします。
5. 「信頼されたルート証明機関」フォルダを右クリックし、[すべてのタスク] > [インポート] を選択して、インポート ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*次へ*をクリックします。
インポート ファイル形式	変更せずに、[次へ] をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、[次へ] をクリックします。
証明書のインポート ウィザードの完了	概要を確認し、[完了] をクリックしてインポートを開始します。



インポートする証明書は秘密キーとバンドルされている必要があります (サポートされている形式は **.pfx**、**.p12**、および ***.p7b** です)。

7. 「個人用」フォルダに対して手順5を繰り返します。

CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための16進数の文字列です。サムプリントは、サムプリント アルゴリズムを使用して証明書の内容から計算されます。

手順

1. GUIで次の手順を実行します。

- a. 証明書をダブルクリックします。
- b. [証明書] ダイアログボックスで、[詳細] タブをクリックします。
- c. フィールドのリストをスクロールして、「拇印」をクリックします。
- d. ボックスから16進数の文字をコピーします。
- e. 16進数の間のスペースを削除します。

たとえば、拇印が「a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b」の場合、スペースを削除すると「a909502dd82ae41433e6f83886b00d4277a32a7b」になります。

2. PowerShellで、次の手順を実行します。

- a. 次のコマンドを実行して、インストールされている証明書のサムプリントを表示し、最近インストールされた証明書をサブジェクト名で識別します。

```
Get-ChildItem -Path 証明書:\LocalMachine\My
```

- b. サムプリントをコピーします。

Windowsホスト プラグイン サービスでのCA証明書の設定

インストールされているデジタル証明書をアクティブ化するには、Windowsホスト プラ

グイン サービスを使用してCA証明書を設定する必要があります。

SnapCenter Serverと、CA証明書がすでに導入されているすべてのプラグイン ホストで、次の手順を実行します。

手順

1. 次のコマンドを実行して、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例えば：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 次のコマンドを実行して、新しくインストールした証明書をWindowsホスト プラグイン
サービスとバインドします。
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例えば：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

プラグインのCA証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインでCA証明書の検証を有効にする必要があります。

開始する前に

- 実行 *Set-SmCertificateSettings* コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- *Get-SmCertificateSettings* を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。

2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. プラグイン ホストを1つまたは複数選択します。
4. *その他のオプション*をクリックします。
5. *証明書の検証を有効にする*を選択します。

終了後の操作

[Managed Hosts] タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Serverとプラグイン ホスト間の接続のステータスを示します。

- *  * は、CA 証明書が有効になっていないか、プラグイン ホストに割り当てられていないことを示します。
- *  * は CA 証明書が正常に検証されたことを示します。
- *  * は、CA 証明書を検証できなかったことを示します。
- *  * は接続情報を取得できなかったことを示します。



ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

SnapCenter Plug-in for VMware vSphereのインストール

データベースまたはファイルシステムが仮想マシン（VM）に格納されている場合や、VMとデータストアを保護する場合は、SnapCenter Plug-in for VMware vSphere仮想アプライアンスを導入する必要があります。

展開方法については、["導入プロセスの概要"](#)。

CA証明書を導入する

SnapCenter Plug-in for VMware vSphereで CA 証明書を構成するには、以下を参照してください。 ["SSL証明書を作成またはインポートする"](#)。

CRLファイルを設定する

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリでCRLファイルを探します。SnapCenter Plug-in for VMware vSphere のCRL ファイルのデフォルト ディレクトリは `/opt/netapp/config/crl` です。

このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

Windowsファイルシステムのバックアップ

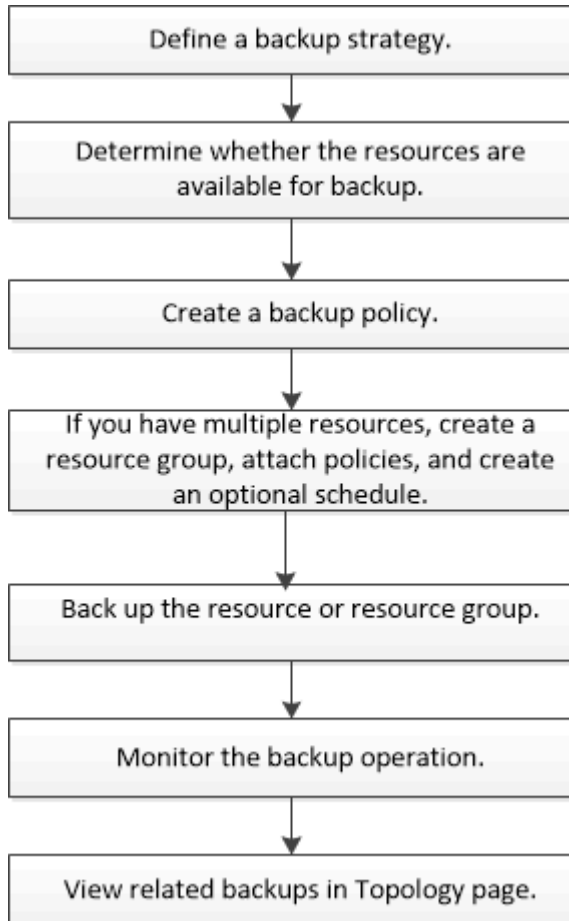
Windowsファイルシステムのバックアップ

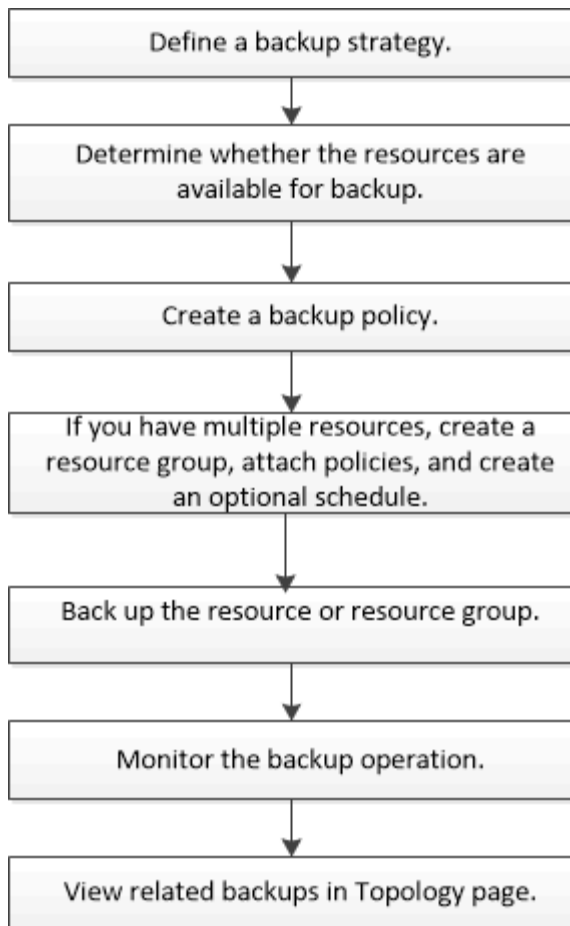
SnapCenter Plug-in for Microsoft Windowsをインストールした環境では、SnapCenterを

使用してWindowsファイルシステムをバックアップすることができます。単一のファイルシステム、または複数のファイルシステムを含むリソースグループをバックアップできます。バックアップは、オンデマンドで実行するか、または定義した保護スケジュールに従って実行できます。

スケジュールを設定して、複数のサーバで同時に複数のバックアップを実行することができます。同じリソースに対してバックアップ処理とリストア処理を同時に実行することはできません。

次のワークフローは、バックアップ処理の実行順序を示しています。





PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。SnapCenterコマンドレットのヘルプまたは ["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#) PowerShell コマンドレットに関する詳細情報が含まれています。

Windows ファイルシステムの使用可能なリソースの確認

リソースとは、インストールしたプラグインで管理されるファイルシステム内のLUNやそれに類するコンポーネントのことです。それらのリソースをリソース グループに追加することで複数のリソースに対してデータ保護ジョブを実行できますが、その前に利用可能なリソースを特定しておく必要があります。利用可能なリソースを検出することで、プラグインのインストールが正常に完了したことの確認にもなります。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、Storage Virtual Machine (SVM) 接続の作成、クレデンシャルの追加などのタスクを完了しておく必要があります。
- ファイルがVMware RDM LUNまたはVMDKにある場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。詳細については、以下を参照してください。 ["SnapCenter Plug-in for VMware vSphereのドキュメント"](#)。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リストから ファイル システム を選択します。

3. リソースのリストをフィルタリングするホストを選択し、[リソースの更新] をクリックします。

新たに追加、名前変更、または削除されたファイルシステムが、SnapCenter Serverのインベントリで更新されます。



SnapCenterの外部でデータベースの名前が変更された場合は、リソースを更新する必要があります。

Windows ファイルシステムのバックアップ ポリシーの作成

SnapCenterを使用してWindows ファイルシステムをバックアップする前に、リソースの新しいバックアップ ポリシーを作成することができます。また、リソース グループの作成時やリソースのバックアップ時に新しいバックアップ ポリシーを作成することも可能です。

開始する前に

- バックアップ戦略を定義しておく必要があります。"[詳細情報](#)"
- データ保護の準備が完了している必要があります。

データ保護の準備として、SnapCenterのインストール、ホストの追加、リソースの検出、Storage Virtual Machine (SVM) 接続の作成などのタスクを完了しておく必要があります。

- Snapshotをミラー セカンダリ ストレージまたはバックアップ セカンダリ ストレージにレプリケートするユーザには、SnapCenter管理者がソースとデスティネーションの両方のボリューム用にSVMを割り当てる必要があります。
- プリスクリプトとポストスクリプトでPowerShellスクリプトを実行する場合は、web.configファイルのUsePowershellProcessforScriptsパラメータの値をtrueに設定する必要があります。

デフォルト値はfalseです。

- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、"[SnapMirrorアクティブ同期のオブジェクト数の制限](#)"。

タスク概要

- SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.ConfigファイルにあるPredefinedWindowsScriptsDirectoryキーを使用して定義します。

必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

キーの値は、API を介して Swagger から表示できます: API /4.7/configsettings

GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。

- SnapLock
 - [Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで指定した保持日数以下にする必要があります。
 - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結

果、ポリシーで指定した数よりも多くのSnapshotが保持される可能性があります。

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] を選択します。
2. [設定] ページで、[ポリシー] を選択します。
3. *新規*を選択します。
4. 「名前」 ページで、ポリシー名と詳細を入力します。
5. 「バックアップとレプリケーション」 ページで、次のタスクを実行します。

- a. バックアップ設定を選択します。

オプション	説明
File System Consistent Backup	ファイルシステムが配置されたディスク ドライブをバックアップ処理の開始前にSnapCenterで休止し、バックアップ処理の終了後に再開する場合は、このオプションを選択します。
File System Crash-consistent Backup	ファイルシステムが配置されたディスク ドライブをSnapCenterで休止しない場合は、このオプションを選択します。

- b. スケジュール頻度（ポリシー タイプ）を選択します。

ポリシーではバックアップの頻度のみを指定します。バックアップの具体的なスケジュールは、リソース グループで定義します。したがって、複数のリソース グループで同じポリシーとバックアップ頻度を使用している場合でも、別々のバックアップ スケジュールを設定できます。



午前 2 時にスケジュールを設定した場合、夏時間 (DST) 中はスケジュールは実行されません。

- c. ポリシーラベルを選択します。

ONTAPによって、選択したSnapshotラベルに一致するセカンダリSnapshotの保持ポリシーが適用されます。



ローカル **Snapshot** コピーの作成後に**SnapMirror**を更新する を選択した場合は、オプションでセカンダリ ポリシー ラベルを指定できます。ただし、ローカル スナップショット コピーの作成後に**SnapVault**を更新する を選択した場合は、セカンダリ ポリシー ラベルを指定する必要があります。

6. [セカンダリ レプリケーション オプションの選択] セクションで、次のセカンダリ レプリケーション オプションの 1 つまたは両方を選択します。

フィールド	操作
Update SnapMirror after creating a local Snapshot copy	別のボリュームにバックアップ セットのミラー コピーを作成する場合（SnapMirror）は、このオプションを選択します。 このオプションは、SnapMirrorアクティブ同期に対して有効にする必要があります。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 見る"Topologyページでの関連するバックアップとクローンの表示"。
Update SnapVault after creating a Snapshot copy	ディスクツーディスクのバックアップ レプリケーションを実行する場合は、このオプションを選択します。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。[Topology]ページの[Refresh]ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリのSnapLock有効期限が更新されます。 SnapLockが（SnapLock Vaultと呼ばれる）ONTAPのセカンダリにのみ設定されている場合は、[Topology]ページの[Refresh]ボタンをクリックすると、ONTAPから取得したセカンダリのSnapLock有効期限が更新されます。 SnapLock Vaultの詳細については、"バックアップ デスティネーションのSnapshotコピーのWORM状態へのコミット"
Error retry count	レプリケーションの最大試行回数を入力します。この回数を超えると処理が停止します。



セカンダリ ストレージでSnapshotの上限に達しないように、ONTAPでセカンダリ ストレージのSnapMirror保持ポリシーを設定する必要があります。

7. [\[保持設定\]](#) ページで、オンデマンド バックアップと選択した各スケジュール頻度の保持設定を指定します。

オプション	説明
保持するスナップショットコピーの合計数	SnapCenterで保持するSnapshotの個数を指定する場合は、このオプションを選択します。指定した個数を超えると自動的に削除されます。
スナップショットコピーを保存する	SnapCenterでバックアップ コピーを保持する日数を指定する場合は、このオプションを選択します。指定した日数を過ぎると削除されます。
スナップショットコピーのロック期間	スナップショットのロック期間を選択し、期間を日数、月数、または年数で指定します。 SnapLock保持期間は100年未満にする必要があります。



保持数は2以上に設定する必要があります。保持数の最小値は2です。



最大保持値は 1018 です。保持期間がONTAPバージョンでサポートされている値よりも高い値に設定されている場合、バックアップは失敗します。

8. [Script]ページで、バックアップ処理の前後にSnapCenter Serverで実行するプリスクリプトやポストスクリプトを入力し、それぞれのスクリプトについてSnapCenterでの実行をタイムアウトするまでの時間を入力します。

たとえば、SNMPトラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。



プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

9. 概要を確認し、[完了] をクリックします。

Windows ファイルシステムのリソース グループの作成

リソース グループとは、保護する複数のファイルシステムを追加できるコンテナです。リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義し、バックアップ スケジュールを指定することも必要です。

タスク概要

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期を使用しない新しいファイルシステムを、SnapMirrorアクティブ同期を使用するリソースを含む既存のリソース グループに追加することはできません。
- SnapMirrorアクティブ同期のフェイルオーバー モードにある既存のリソース グループに新しいファイルシステムを追加することはできません。リソースを追加できるのは、通常の状態またはフェイルバック状態のリソース グループのみです。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リストから ファイル システム を選択します。



最近SnapCenterにファイル システムを追加した場合は、[リソースの更新] をクリックして、新しく追加されたリソースを表示します。

3. *新しいリソース グループ*をクリックします。
4. ウィザードの[Name]ページで、次の操作を実行します。

フィールド	操作
Name	リソース グループ名を入力します。  リソース グループ名は250文字以内で指定する必要があります。
Use custom name format for Snapshot copy	オプション: カスタム スナップショットの名前と形式を入力します。 たとえ ば、customtext_resourcegroup_policy_hostname やresourcegroup_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。
Tag	リソース グループを検索するときに役立つわかりやすいタグを入力します。

5. [Resources]ページで、次の作業を実行します。
 - a. ホストを選択してリソースのリストをフィルタリングします。

最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources]のリストには表示されません。
 - b. [Available Resources]セクションでバックアップするファイルシステムをクリックし、右矢印をクリックして[Added]セクションに移動します。

同じストレージ ボリューム上のすべてのリソースを自動選択 オプションを選択すると、同じボリューム上のすべてのリソースが選択されます。その状態で[Added]セクションに移動した場合、そのボリュームのすべてのリソースが一緒に移動されます。

単一のファイル システムを追加するには、[同じストレージ ボリューム上のすべてのリソースを自動選択する] オプションをオフにし、[追加済み] セクションに移動するファイル システムを選択します。
6. [Policies]ページで、次の作業を実行します。
 - a. ドロップダウン リストから1つ以上のポリシーを選択します。

既存のポリシーを選択し、「詳細」をクリックして、そのポリシーを使用できるかどうかを判断できます。

既存のポリシーが要件を満たしていない場合は、 をクリックして新しいポリシーを作成できます。
* ポリシー ウィザードを起動します。

選択したポリシーが[Configure schedules for selected policies]セクションの[Policy]列に表示されます。

- b. 選択したポリシーのスケジュールを構成するセクションで、 * スケジュールを構成するポリシーの [スケジュールの構成] 列で、
- c. ポリシーが複数のスケジュール タイプ（頻度）に関連付けられている場合は、設定する頻度を選択します。
- d. [ポリシー *policy_name* のスケジュールの追加] ダイアログ ボックスで、開始日、有効期限、頻度を指定してスケジュールを構成し、[完了] をクリックします。

設定したスケジュールは、[Configure schedules for selected policies]セクションの[Applied Schedules]列に表示されます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。Windowsタスク スケジューラとSQL Server Agentからスケジュールを変更しないでください。

7. [Notification]ページで、通知の情報を次のように指定します。

フィールド	操作
メール設定	バックアップ リソース グループを作成し、ポリシーを添付し、スケジュールを構成した後、受信者に電子メールを送信するには、[常に]、[失敗時]、または [失敗または警告時] を選択します。SMTPサーバ、Eメールのデフォルトの件名、および送信先と送信元のEメール アドレスを入力します。
から	Eメール アドレス
To	Eメールの送信先アドレス
Subject	Eメールのデフォルトの件名

8. 概要を確認し、[完了] をクリックします。

オンデマンドでバックアップを実行できるほか、スケジュールに従ってバックアップが開始されます。

ASA r2 システム上の Windows ファイル システムのリソース グループを作成し、二次保護を有効にします。

ASA r2 システム上にあるリソースを追加するには、リソース グループを作成する必要があります。リソース グループの作成時にセカンダリ保護をプロビジョニングすることもできます。

開始する前に

- ONTAP 9.x リソースとASA r2 リソースの両方を同じリソース グループに追加していないことを確認する必要があります。
- ONTAP 9.x リソースとASA r2 リソースの両方を含むデータベースが存在しないことを確認する必要があります。

タスク概要

- 二次保護は、ログインしたユーザーに **SecondaryProtection** 機能が有効になっているロールが割り当てられている場合にのみ使用できます。
- セカンダリ保護を有効にすると、プライマリおよびセカンダリ整合性グループの作成中にリソース グループはメンテナンス モードになります。プライマリおよびセカンダリのコンシステンシー グループが作成されると、リソース グループのメンテナンス モードが解除されます。
- SnapCenter はクローン リソースの二次保護をサポートしていません。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。

- a. [Name] フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag] フィールドに1つ以上のラベルを入力します。

たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

- c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- d. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。



必要に応じて、プレフィックスを含め、アプリケーションで設定されたのと同じ宛先を使用する必要があります。

4. [リソース] ページで、[ホスト] ドロップダウン リストからデータベース ホスト名を選択します。



[Available Resources] セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources] のリストには表示されません。

5. [使用可能なリソース] セクションからASA r2 リソースを選択し、[選択したリソース] セクションに移動します。
6. アプリケーション設定ページで、バックアップ オプションを選択します。
7. [Policies]ページで、次の手順を実行します。
 - a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックし  でポリシーを作成することもできます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、  をクリックします。
- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 選択したポリシーに対して二次保護が有効になっている場合は、「二次保護」 ページが表示されるので、次の手順を実行する必要があります。
 - a. レプリケーション ポリシーのタイプを選択します。



同期レプリケーション ポリシーはサポートされていません。

- b. 使用する整合性グループのサフィックスを指定します。
- c. [宛先クラスタ] および [宛先 SVM] ドロップダウンから、使用するピア クラスタと SVM を選択します。



クラスタと SVM のピアリングはSnapCenterではサポートされていません。クラスタと SVM のピアリングを実行するには、System Manager またはONTAP CLI を使用する必要があります。



リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは [セカンダリ保護リソース] セクションに表示されます。

1. [Verification]ページで、次の手順を実行します。
 - a. ロケータのロード をクリックして、 SnapMirrorまたはSnapVaultボリュームをロードし、セカンダリストレージで検証を実行します。
 - b. クリック  ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で をクリックします。

- c. [Add Verification Schedules policy_name]ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

- d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証]を選択します。
- e. [OK]をクリックします。

設定した検証スケジュールが、[Applied Schedules]列にリストされます。

2. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

3. 概要を確認し、[完了] をクリックします。

PowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成

PowerShellコマンドレットを使用してデータ保護処理を実行するには、Storage Virtual Machine (SVM) 接続とクレデンシャルを作成しておく必要があります。

開始する前に

- PowerShellコマンドレットを実行できるようにPowerShell環境を準備しておく必要があります。
- ストレージ接続を作成するには、Infrastructure Adminロールの権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

ストレージ システム接続の追加中は、ホスト プラグインのインストールが進行中であってはなりません。ホスト キャッシュが更新されず、SnapCenter GUI にデータベースのステータスが「バックアップに使用できません」または「NetAppストレージ上にありません」と表示される可能性があるためです。

- ストレージ システムの名前は一意である必要があります。

SnapCenterでは、別々のクラスタに属している場合でも、複数のストレージ システムに同じ名前を付けることはサポートされません。SnapCenterでサポートする各ストレージ システムには、一意な名前と管理LIFの一意なIPアドレスが必要です。

手順

1. Open-SmConnection コマンドレットを使用して、PowerShell Core 接続セッションを開始します。

PowerShell セッションを開く例を次に示します。

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

2. Add-SmStorageConnection コマンドレットを使用して、ストレージ システムへの新しい接続を作成します。

新しいストレージ システム接続を作成する例を次に示します。

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Add-SmCredential コマンドレットを使用して、新しいクレデンシャルを作成します。

Windows クレデンシャルを使用して FinanceAdmin という名前の新しいクレデンシャルを作成する例を次に示します。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

コマンドレットで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenter ソフトウェア コマンドレット リファレンス ガイド](#)"。

Windows ファイルシステムの単一リソースのオンデマンド バックアップ

リソース グループに含まれていないリソースは、[Resources] ページからオンデマンドでバックアップすることができます。

タスク概要

セカンダリ ストレージとの SnapMirror 関係を持つリソースをバックアップする場合、ストレージ ユーザーに割り当てられているロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。



SnapCenter によるファイルシステムのバックアップでは、バックアップするファイルシステムのボリューム マウント ポイント (VMP) にマウントされている LUN はバックアップされません。



Windows ファイルシステムについての作業では、データベース ファイルはバックアップしないでください。バックアップを作成しても整合性に欠け、リストア時にデータが失われる可能性があります。データベース ファイルを保護するには、データベースに適した SnapCenter プラグイン (たとえば、Microsoft SQL Server 用の SnapCenter プラグインや Microsoft Exchange Server 用の SnapCenter プラグインなど) を使用する必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [Resources] ページで、リソース タイプとして [File System] を選択し、バックアップするリソースを選択します。
3. ファイル システム - 保護ウィザードが自動的に起動しない場合は、[保護] をクリックしてウィザードを起動します。

「リソース グループの作成」の作業の説明に従って、保護設定を指定します。

4. オプション: ウィザードのリソース ページで、スナップショットのカスタム名形式を入力します。

たとえば、`customtext_resourcegroup_policy_hostname`や`resourcegroup_hostname`などの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

5. [Policies] ページで、次の作業を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。

既存のポリシーを選択し、[詳細] をクリックして、そのポリシーを使用できるかどうかを確認できます。

既存のポリシーがいずれも要件を満たさない場合は、既存のポリシーをコピーして変更する

か、 をクリックしてポリシー ウィザードで新しいポリシーを作成できます。既存のポリシ

ーがいずれも要件を満たさない場合は、既存のポリシーをコピーして変更するか、 をクリックしてポリシー ウィザードで新しいポリシーを作成できます。

選択したポリシーが [Configure schedules for selected policies] セクションの [Policy] 列に表示されます。

- b. 選択したポリシーのスケジュールを構成するセクションで、 スケジュールを構成するポリシーの [スケジュールの構成] 列で、
- c. [ポリシー *policy_name* のスケジュールの追加] ダイアログ ボックスで、開始日、有効期限、頻度を指定してスケジュールを構成し、[完了] をクリックします。

設定したスケジュールは、[Configure schedules for selected policies] セクションの [Applied Schedules] 列に表示されます。

"スケジュールを設定した処理は失敗することがあります。"

6. [Notification] ページで、次の作業を行います。

フィールド	操作
メール設定	バックアップ リソース グループを作成し、ポリシーを添付し、スケジュールを構成した後、受信者に電子メールを送信するには、[常に]、[失敗時]、または [失敗または警告時] を選択します。 SMTP サーバー情報、デフォルトの電子メール 件名、および「To」 および「From」 電子メール アドレスを入力します。
から	Eメール アドレス
To	Eメールの送信先アドレス
Subject	Eメールのデフォルトの件名

7. 概要を確認し、[完了] をクリックします。

データベース トポロジのページが表示されます。

8. *今すぐバックアップ*をクリックします。

9. [Backup]ページで次の手順を実行します。

- リソースに複数のポリシーを適用した場合は、バックアップに使用するポリシーを[Policy]ドロップダウン リストから選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- *バックアップ*をクリックします。

10. モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレット

手順

- Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

ユーザ名とパスワードのプロンプトが表示されます。

- Add-SmPolicyコマンドレットを使用して、バックアップ ポリシーを作成します。

この例では、SQLのバックアップ タイプ「FullBackup」を指定して新しいバックアップ ポリシーを作成しています。

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

この例では、Windowsファイルシステムのバックアップ タイプ「CrashConsistent」を指定して新しいバックアップ ポリシーを作成しています。

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Get-SmResourcesコマンドレットを使用してホスト リソースを検出します。

この例では、指定したホスト上でMicrosoft SQLプラグインのリソースを検出しています。

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

この例では、指定したホスト上でWindowsファイルシステムのリソースを検出しています。

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Add-SmResourceGroupコマンドレットを使用して、SnapCenterに新しいリソース グループを追加します。

この例では、ポリシーとリソースを指定して新しいSQLデータベース バックアップ リソース グループを作成しています。

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

この例では、ポリシーとリソースを指定して新しいWindowsファイルシステム バックアップ リソース グループを作成しています。

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```


5. New-SmBackupコマンドレットを使用して、新しいバックアップ ジョブを開始します。

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy FinancePolicy
```

6. Get-SmBackupReportコマンドレットを使用して、バックアップ ジョブのステータスを表示します。

この例では、指定した日に実行されたすべてのジョブの概要レポートを表示しています。

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

Windows ファイルシステムのリソース グループのバックアップ

リソース グループは、ホストまたはクラスタ上のリソースの集まりです。リソース グループのバックアップ処理は、リソース グループに定義されているすべてのリソースを対象に実行されます。リソース グループは、[Resources] ページからオンデマンドでバックアップできます。リソース グループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが行われます。

開始する前に

- ポリシーを適用したリソース グループを作成しておく必要があります。
- セカンダリ ストレージにSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられているロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。
- リソース グループにホストが異なる複数のデータベースが含まれている場合、一部のホストではネットワークの問題が原因でバックアップ処理のトリガーに時間がかかることがあります。PowerShell コマンドレット Set-SmConfigSettings を使用して、web.config で MaxRetryForUninitializedHosts の値を設定する必要があります。



SnapCenterによるファイルシステムのバックアップでは、バックアップするファイルシステムのボリューム マウント ポイント (VMP) にマウントされているLUNはバックアップされません。



Windowsファイルシステムについての作業では、データベース ファイルはバックアップしないでください。バックアップを作成しても整合性に欠け、リストア時にデータが失われる可能性があります。データベース ファイルを保護するには、データベースに適したSnapCenterプラグイン (たとえば、Microsoft SQL Server 用のSnapCenterプラグインや Microsoft Exchange Server 用のSnapCenterプラグインなど) を使用する必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。

2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。

リソース グループを検索することができます。そのためには、検索ボックスにリソース グループ名を入力するか、をクリックし、タグを選択します。そのあとにをクリックすると、フィルタ ペインが閉じます。

3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] をクリックします。



SnapCenter Plug-in for Oracle Databaseでは、2つのデータベースが統合されたリソース グループがある場合に、一方のデータベースのデータファイルがNetApp以外のストレージにあると、もう一方のデータベースがNetAppストレージにあっても、バックアップ処理は中止されます。

4. [Backup] ページで次の手順を実行します。

- a. リソース グループに複数のポリシーを関連付けている場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*をクリックします。

5. モニター > ジョブ をクリックして、操作の進行状況を監視します。

- MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

"MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"

- VMDK上のアプリケーション データをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープ サイズが不足していると、バックアップが失敗することがあります。Java ヒープサイズを増やすには、スクリプトファイルを見つけます。

/opt/netapp/init_scripts/scvservice。その脚本では、do_start method`コマンドは、SnapCenter VMware プラグイン サービスを開始します。このコマンドを次のように更新します。
`Java -jar -Xmx8192M -Xms4096M。

バックアップ処理の監視

SnapCenterの[Jobs]ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

-  進行中
-  正常に完了しました
-  失敗した

-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*ジョブ*をクリックします。
3. [Jobs]ページで、次の手順を実行します。
 - a. をクリックして、 リストの内容をバックアップ処理だけに絞り込みます。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*バックアップ*を選択します。
 - d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. バックアップ ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスは  ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[Activity]ペインでの処理の監視

[Activity]ペインには、最後に実行された5つの処理が表示されます。また[Activity]ペインには、処理が開始された日次と処理のステータスが表示されます。

[Activity]ペインには、バックアップ、リストア、クローニング、スケジュールされたバックアップの各処理に関する情報が表示されます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. クリック  アクティビティ ペインで、最新の 5 つの操作を表示します。

いずれかの操作をクリックすると、*ジョブの詳細*ページに操作の詳細が表示されます。

バックアップ処理のキャンセル

キューに登録されているバックアップ処理はキャンセルできます。

必要なもの

- 処理をキャンセルするには、SnapCenter管理者がジョブ所有者としてログインする必要があります。
- バックアップ操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のバックアップ処理はキャンセルできません。
- バックアップ処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。
- キャンセルできない操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたバックアップ操作をキャンセルできます。

手順

1. 次のいずれかを実行します。

方法	アクション
[Monitor]ページ	a. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 b. 操作を選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	a. バックアップ操作を開始したら、*をクリックします。 * アクティビティ ペインで、最新の 5 つの操作を表示します。 b. 処理を選択します。 c. ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

処理がキャンセルされ、リソースは処理前の状態に戻ります。

[Topology]ページでの関連するバックアップとクローンの表示

リソースのバックアップまたはクローニングを準備する際に、プライマリ ストレージとセカンダリ ストレージ上のすべてのバックアップとクローンの図を表示できます。[Topology]ページでは、選択したリソースまたはリソース グループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を参照し、対象を選択してデータ保護処理を実行できます。

タスク概要

プライマリ ストレージまたはセカンダリ ストレージ（ミラー コピーまたはバックアップ コピー）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

•



プライマリ ストレージで使用可能なバックアップとクローンの数を表示します。



SnapMirrorテクノロジーを使用してセカンダリ ストレージにミラーリングされているバックアップとクローンの数を表示します。



mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンもトポロジ ビューに表示されますが、トポロジ ビューのミラー バックアップの数には、バージョンに依存しないバックアップが含まれません。



SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップとクローンの数を表示します。

- 表示されるバックアップの数には、セカンダリ ストレージから削除されたバックアップも含まれます。たとえば、4個のバックアップのみを保持するポリシーを使用して6個のバックアップを作成した場合、バックアップの数は6個と表示されます。



mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンもトポロジ ビューに表示されますが、トポロジ ビューのミラー バックアップの数には、バージョンに依存しないバックアップが含まれません。

SnapMirrorアクティブ同期 (当初はSnapMirror Business Continuity [SM-BC] としてリリース) としてセカンダリ関係がある場合は、次の追加アイコンが表示されます。



レプリカサイトが稼働しています。



レプリカサイトはダウンしています。



セカンダリ ミラーまたはボルト関係が再確立されていません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストからリソースまたはリソース グループを選択します。
3. リソースの詳細ビューまたはリソース グループの詳細ビューで、リソースを選択します。

リソースが保護されている場合は、選択したリソースのトポロジ ページが表示されます。

4. [Summary Card]で、プライマリ ストレージとセカンダリ ストレージ上にあるバックアップとクローンの数の概要を確認します。

[Summary Card]セクションには、バックアップとクローンの総数が表示されます。Oracleデータベースについては、[Summary Card]セクションにログ バックアップの総数も表示されます。

更新 ボタンをクリックすると、ストレージのクエリが開始され、正確な数が表示されます。

SnapLock対応バックアップが取得された場合、[更新] ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでも、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

アプリケーション リソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限はONTAPから取得されます。

SnapMirrorアクティブ同期の場合、[更新] ボタンをクリックすると、プライマリ サイトとレプリカ サイトの両方に対してONTAP を照会してSnapCenterバックアップ インベントリが更新されます。週次スケジュールでも、SnapMirrorアクティブ同期関係を含むすべてのデータベースに対してこの処理が実行されます。

- SnapMirrorアクティブ同期とONTAP（バージョン9.14.1のみ）では、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップの関係については、フェイルオーバー後に手動で設定する必要があります。ONTAP 9.15.1以降は、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップが、自動的に設定されます。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。バックアップが作成された後にのみ、「更新」をクリックできます。

5. 「コピーの管理」ビューで、プライマリ ストレージまたはセカンダリ ストレージから バックアップ または クローン をクリックして、バックアップまたはクローンの詳細を表示します。

バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、名前変更、削除の各処理を実行します。

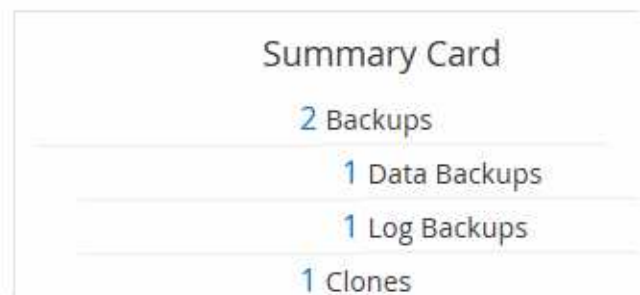
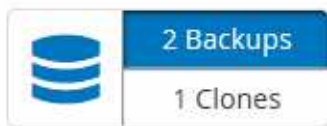


セカンダリ ストレージ システム上のバックアップは、名前変更または削除できません。

7. クローンを削除する場合は、表でクローンを選択し、 をクリックして削除します。

プライマリ ストレージのバックアップとクローンの例

Manage Copies



PowerShellコマンドレットを使用したセカンダリ バックアップ数のクリーンアップ

Remove-SmBackupコマンドレットを使用して、Snapshotがないセカンダリ バックアップのバックアップ数をクリーンアップできます。コピーの管理トポロジに表示されるスナップショットの合計がセカンダリ ストレージのスナップショット保持設定と一致しない場合に、このコマンドレットを使用することをお勧めします。

PowerShellコマンドレットを実行できるように環境を準備しておく必要があります。

コマンドレットで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると

取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-SmConnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. -CleanupSecondaryBackupsパラメータを使用してセカンダリ バックアップ数をクリーンアップします。

この例では、Snapshotがないセカンダリ バックアップのバックアップ数をクリーンアップしています。

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s) .
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Windows ファイルシステムのリストア

Windows ファイルシステムのバックアップのリストア

SnapCenterを使用してファイルシステムのバックアップをリストアすることができます。ファイルシステムのリストアは、指定したバックアップのすべてのデータをファイルシステムの元の場所にコピーする複数の段階からなるプロセスです。

開始する前に

- ファイルシステムをバックアップしておく必要があります。
- ファイルシステムに対してバックアップ処理などのスケジュールが設定された処理が現在進行している場合は、リストア処理を開始する前にキャンセルしておく必要があります。
- ファイルシステムのバックアップは元の場所にのみリストアできます。別のパスを指定することはできません。

ファイルシステムのリストアでは、ファイルシステムの元の場所にあるデータがすべて上書きされ、バックアップからファイル単位でリストアすることはできません。ファイルシステムのバックアップに含まれる単一のファイルをリストアするには、バックアップをクローニングし、クローン内のファイルを使用する必要があります。

- システム ボリュームやブート ボリュームはリストアできません。
- SnapCenterでは、クラスタ グループをオフラインにすることなく、Windowsクラスタのファイルシステムをリストアできます。

タスク概要

- SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.Configファイルにあ

るPredefinedWindowsScriptsDirectoryキーを使用して定義します。

必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

キーの値は、API を介して Swagger から表示できます: [API /4.7/configsettings](#)

GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。

- SnapMirrorアクティブ同期でリストア処理を実行するには、プライマリの場所からバックアップを選択する必要があります。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. リソースのリストをフィルタリングするには、[File System]および[Resource Group]のオプションを選択します。
3. リストからリソース グループを選択し、[復元] をクリックします。
4. [Backups]ページで、プライマリとセカンダリのどちらのストレージ システムからリストアするかを選択し、リストアするバックアップを選択します。
5. [Restore]ウィザードで目的のオプションを選択します。
6. リストア処理の実行前や実行後にSnapCenterで実行するプリスクリプトやポストスクリプトのパスと引数を入力できます。

たとえば、SNMPトラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。



プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

7. [Notification]ページで、次のいずれかのオプションを選択します。

フィールド	操作
Log SnapCenter server events to storage system syslog	SnapCenter Serverのイベントをストレージ システムのsyslogに記録する場合は、このオプションを選択します。
Send AutoSupport notification for failed operations to storage system	失敗した処理に関する情報をAutoSupportを使用してNetAppに送信する場合は、このオプションを選択します。
メール設定	バックアップの復元後に受信者に電子メールメッセージを送信するには、「常時」、「失敗時」、または「失敗または警告時」を選択します。SMTPサーバ、Eメールのデフォルトの件名、および送信先と送信元のEメール アドレスを入力します。

8. 概要を確認し、[完了] をクリックします。
9. モニター > ジョブ をクリックして、操作の進行状況を監視します。



リストアしたファイルシステムにデータベースが含まれている場合は、データベースもリストアする必要があります。データベースをリストアしないと、データベースが無効な状態になることがあります。データベースのリストアの詳細については、そのデータベースのデータ保護ガイドを参照してください。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよびGet-SmBackupReportコマンドレットを使用して、リストアする1つまたは複数のバックアップに関する情報を取得します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackupコマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

PowerShellコマンドレットを使用したリソースのリストア

リソースのバックアップをリストアするときは、SnapCenter Serverとの接続セッションを開始し、バックアップをリストしてバックアップの情報を取得し、バックアップをリストアします。

PowerShellコマンドレットを実行できるように環境を準備しておく必要があります。

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよびGet-SmBackupReportコマンドレットを使用して、リストアする1つまたは複数のバックアップに関する情報を取得します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName        : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName        : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. Restore-SmBackupコマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

リストア処理の監視

[Job]ページを使用して、SnapCenterの各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中

-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  てリストをフィルタリングし、リストア処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*復元*を選択します。
 - d. *ステータス*ドロップダウンリストから、復元ステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. 復元ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

リストア処理のキャンセル

キューに登録されているリストア ジョブはキャンセルできます。

リストア処理をキャンセルするには、SnapCenter管理者かジョブ所有者としてログインする必要があります。

タスク概要

- キューに入れられた復元操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のリストア処理はキャンセルできません。
- キューに登録されているリストア処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。
- キャンセルできない復元操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられた復元操作をキャンセルできます。

手順

次のいずれかを実行します。

方法	アクション
[Monitor]ページ	1. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 2. ジョブを選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	1. 復元操作を開始したら、 アクティビティ ペインで、最新の 5 つの操作を表示します。 2. 処理を選択します。 3. ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

Windows ファイルシステムのクローニング

Windows ファイルシステムのバックアップからのクローニング

SnapCenterを使用してWindowsファイルシステムのバックアップをクローニングすることができます。誤って削除または変更された単一のファイルのコピーが必要な場合は、バックアップをクローニングし、クローン内のファイルを使用できます。

開始する前に

- データ保護の準備として、ホストの追加、リソースの特定、Storage Virtual Machine (SVM) 接続の作成などのタスクを完了しておく必要があります。
- ファイルシステムのバックアップを作成しておく必要があります。
- ボリュームをホストするアグリゲートがStorage Virtual Machine (SVM) の割り当て済みアグリゲート リストに含まれていることを確認します。
- リソース グループはクローニングできません。クローニングできるのは、個々のファイルシステムのバックアップだけです。
- SnapCenterでは、VMDKディスクを使用した仮想マシン上にあるバックアップを物理サーバにクローニングすることはできません。
- 共有LUNやクラスタ共有ボリューム (CSV) LUNなどのWindowsクラスタをクローニングした場合、クローンは指定したホストに専用のLUNとして格納されます。
- クローニング処理では、ボリューム マウント ポイントのルート ディレクトリを共有ディレクトリにすることはできません。
- クローンはアグリゲートのホーム ノード以外のノードには作成できません。
- Windowsファイルシステムのクローニング処理では、定期的なスケジュール (クローン ライフサイクル) は設定できません。バックアップのクローニングはオンデマンドでのみ実行できます。
- クローンが含まれているLUNを新しいボリュームに移動すると、SnapCenterでそのクローンをサポートできなくなります。たとえば、SnapCenterでそのクローンを削除できなくなります。
- 複数の環境間でのクローニングは実行できません。例：物理ディスクから仮想ディスクへ、またはその逆のクローニングなど。

タスク概要

- SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.ConfigファイルにあるPredefinedWindowsScriptsDirectoryキーを使用して定義します。

必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

キーの値は、API を介して Swagger から表示できます: API /4.7/configsettings

GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リストから ファイル システム を選択します。
3. ホストを選択します。

リソースが保護されていれば、トポロジ ビューが自動的に表示されます。

4. リソース リストからクローニングするバックアップを選択し、クローン アイコンをクリックします。
5. [Options] ページで、次の操作を実行します。

フィールド	操作
Clone server	クローンをどのホスト上に作成するかを選択します。
「マウント ポイントの自動割り当て」または「パスの下ボリューム マウント ポイントの自動割り当て」	マウント ポイントを自動的に割り当てるか、またはパスを指定してボリューム マウント ポイントを自動的に割り当てるかを選択します。 パスの下ボリューム マウント ポイントを自動割り当て: パスの下のマウント ポイントを使用すると、マウント ポイントが作成される特定のディレクトリを指定できます。このオプションを選択する場合は、ディレクトリが空であることを事前に確認しておく必要があります。ディレクトリにバックアップが格納されている場合、そのバックアップはマウント処理後に無効な状態になります。
Archive location	セカンダリ バックアップをクローニングする場合にアーカイブの場所を選択します。

6. [Script] ページで、実行するプリスクリプトやポストスクリプトがあれば指定します。



プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

7. 概要を確認し、[完了] をクリックします。
8. モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

- クローニングできるバックアップの一覧を表示するには、Get-SmBackupコマンドレットかGet-SmResourceGroupコマンドレットを使用します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

この例では、指定したリソース グループとそのリソース、および関連ポリシーに関する情報を表示しています。

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
```

SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :

```

SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False

```

3. 既存のバックアップからのクローニング処理を開始するには、New-SmCloneコマンドレットを使用します。

この例では、指定したバックアップからすべてのログを含めてクローンを作成しています。

```

PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

この例では、指定したMicrosoft SQL Serverインスタンスのクローンを作成しています。

```
PS C:\> New-SmClone
-B BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-R Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-A AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-S Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"
```

4. クローニング ジョブのステータスを表示するには、Get-SmCloneReport コマンドレットを使用します。

この例では、指定したジョブIDのクローン レポートを表示しています。

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

クローニング処理の監視

SnapCenterのクローニング処理の進捗状況を、[Jobs]ページで監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  てリストをフィルタリングし、クローニング処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*クローン*を選択します。
 - d. *ステータス*ドロップダウンリストからクローンのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. クローンジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. ジョブの詳細ページで、*ログの表示*をクリックします。

クローニング処理のキャンセル

キューに登録されているクローニング処理はキャンセルできます。

クローニング処理をキャンセルするには、SnapCenter管理者かジョブ所有者としてログインする必要があります。

タスク概要

- キューに入れられたクローン操作は、モニター ページまたは アクティビティ ペインからキャンセルできます。
- 実行中のクローニング処理はキャンセルできません。
- キューに登録されているクローニング処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたクローン操作をキャンセルできます。

手順

次のいずれかを実行します。

方法	アクション
[Monitor]ページ	1. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 2. 操作を選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	1. クローン操作を開始したら、 アクティビティ ペインで、最新の 5 つの操作を表示します。 2. 処理を選択します。 3. *ジョブの詳細*ページで、*ジョブのキャンセル* をクリックします。

クローンのスプリット

SnapCenterを使用して、クローン リソースを親リソースからスプリットできます。スプリットされたクローンは親リソースから独立します。

タスク概要

- 中間クローンではクローン スプリット処理を実行できません。

たとえば、データベース バックアップからクローン1を作成したあとで、クローン1のバックアップを作成し、そのバックアップ（クローン2）をクローニングできます。クローン2を作成すると、クローン1は中間クローンになり、クローン1ではクローン スプリット処理を実行できなくなります。ただし、クローン2に対してはクローン スプリット処理を実行できます。

クローン2をスプリットすると、クローン1は中間クローンではなくなるため、クローン1に対してクローン スプリット処理を実行できるようになります。

- クローンをスプリットすると、そのクローンのバックアップ コピーとクローン ジョブが削除されます。
- FlexCloneボリューム分割操作の詳細については、以下を参照してください。 ["親ボリュームからのFlexCloneボリュームのスプリット"](#)。
- ストレージ システム上のボリュームまたはアグリゲートがオンラインであることを確認します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. *リソース*ページで、表示リストから適切なオプションを選択します。

オプション	説明
データベース アプリケーションの場合	表示リストから*データベース*を選択します。
ファイルシステムの場合	表示リストから*パス*を選択します。

3. リストから適切なリソースを選択します。

リソースのトポロジ ページが表示されます。

4. *コピーの管理*ビューから、クローンされたリソース（データベースやLUNなど）を選択し、*をクリックします。  *。
5. 分割するクローンの推定サイズとアグリゲート上で必要な空き容量を確認し、[開始] をクリックします。
6. モニター > ジョブ をクリックして、操作の進行状況を監視します。

SMCoreサービスが再起動されると、クローン スプリット処理は応答を停止します。Stop-SmJobコマンドレットを実行してクローン スプリット処理を停止してから、クローン スプリット処理を再試行してください。

クローンが分割されているかどうかを確認するためのポーリング時間を長くしたり短くしたりする場合は、*SMCoreServiceHost.exe.config* ファイルの *CloneSplitStatusCheckPollTime* パラメータの値を変更して、SMCore がクローン分割操作のステータスをポーリングする時間間隔を設定できます。値はミリ秒単位で、デフォルト値は5分です。

例えば：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

バックアップ、リストア、または別のクローン スプリットが実行中の場合、クローン スプリットの開始処理は失敗します。クローン スプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

["アグリゲートが存在しないためにSnapCenterのクローニングや検証が失敗する"](#)

Microsoft Exchange Serverデータベースの保護

SnapCenter Plug-in for Microsoft Exchange Serverの概念

SnapCenter Plug-in for Microsoft Exchange Serverの概要

SnapCenter Plug-in for Microsoft Exchange Serverは、Exchangeデータベースに対するアプリケーション対応データ保護管理を可能にする、NetApp SnapCenterソフトウェアのホスト側コンポーネントです。Plug-in for Exchangeを使用すると、SnapCenter環境でのExchangeデータベースのバックアップとリストアが自動化されます。

Plug-in for Exchangeをインストールすると、SnapCenterでNetApp SnapMirrorテクノロジーを使用して別のボリュームにバックアップセットのミラー コピーを作成できるほか、NetApp SnapVaultテクノロジーを使用して標準への準拠やアーカイブを目的としたディスクツーディスク バックアップ レプリケーションを実行できます。

Exchangeデータベース全体ではなく、メールやメールボックスの単位でリストアとリカバリを実行する場合は、Single Mailbox Recovery (SMBR) ソフトウェアを使用できます。NetApp® Single Mailbox Recoveryは、2023年5月12日に販売終了 (EOA) になりました。2020年6月24日に導入された販売用パーツ番号を通じてメールボックスの容量、メンテナンス、サポートを購入されたお客様には、サポート対象の期間中は引き続きサポートを提供いたします。

NetApp Single Mailbox Recoveryは、Ontrackが提供するパートナー製品です。Ontrack PowerControlsには、NetApp Single Mailbox Recoveryと同様の機能が用意されています。お客様は、新しいOntrack PowerControlsソフトウェア ライセンスとOntrack PowerControlsのメンテナンスおよびサポート更新をOntrackから (licensingteam@ontrack.com経由で) 購入して、メールボックスをきめ細かくリカバリできます。

Exchange 用プラグインは、サイト全体に障害が発生した場合でもビジネス サービスの運用を継続できるようにするSnapMirrorアクティブ シンク (当初はSnapMirror Business Continuity [SM-BC] としてリリース) をサポートし、セカンダリ コピーを使用してアプリケーションを透過的にフェイルオーバーできるようにします。SnapMirrorアクティブ同期でフェイルオーバーをトリガーするために、手動操作や追加のスクリプト作成は必要ありません。

SnapMirrorアクティブ同期の非対称モード、フェイルオーバー モード、または非二重モードがサポートされます。これは、最適パスがプライマリ側のLUNの所有者ノードからのみであるソリューションを意味します。セカンダリ クラスタ パス上のI/Oは、プロキシ経由でプライマリ クラスタに提供されます。同期レプリケーションは、プライマリからセカンダリへの一方向です。

- SnapCenter環境のMicrosoft Exchange Serverデータベースとデータベース可用性グループ (DAG) に対するアプリケーション対応のバックアップとリストアの各処理が自動化されます。
- SnapCenter Plug-in for VMware vSphereを展開し、そのプラグインをSnapCenterに登録すると、RDM LUN 上の仮想化された Exchange Server がサポートされます。

SnapCenter Plug-in for Microsoft Exchange Serverの機能

Plug-in for Exchangeを使用すれば、Exchange Serverデータベースのバックアップとリストアを実行できます。

- Exchangeデータベース可用性グループ（DAG）、データベース、レプリカ セットのアクティブなインベントリの表示と管理
- バックアップを自動化するための保護設定を可能にするポリシーの定義
- リソース グループへのポリシーの割り当て
- 個々のDAGとデータベースの保護
- プライマリおよびセカンダリExchangeメールボックス データベースのバックアップ
- プライマリおよびセカンダリ バックアップからのデータベースのリストア

SnapCenter Plug-in for Microsoft WindowsおよびSnapCenter Plug-in for Microsoft Exchange Serverでサポートされるストレージ タイプ

SnapCenterは、物理マシンと仮想マシンの両方でさまざまなストレージ タイプをサポートしています。ホストに対応したパッケージをインストールする前に、ストレージ タイプがサポートされているかどうかを確認する必要があります。

Windows Serverでは、SnapCenterによるプロビジョニングとデータ保護がサポートされます。サポートされているバージョンに関する最新情報については、<https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT> [NetApp相互運用性マトリックス ツール]。

マシン	ストレージ タイプ	プロビジョニングを使用して	サポートノート
物理サーバ	FC接続LUN	SnapCenterのグラフィカル ユーザ インターフェイス（GUI）またはPowerShellコマンドレット	
物理サーバ	iSCSI接続LUN	SnapCenterのGUIまたはPowerShellコマンドレット	
VMware VM	FCまたはiSCSI HBAで接続されたRDM LUN	PowerShellコマンドレット	物理的互換性のみ  VMDKはサポートされません。
VMware VM	iSCSIイニシエータでゲスト システムに直接接続されたiSCSI LUN	SnapCenterのGUIまたはPowerShellコマンドレット	 VMDKはサポートされません。

マシン	ストレージ タイプ	プロビジョニングを使用して	サポートノート
Hyper-V VM	仮想ファイバチャネル スイッチで接続された仮想FC (vFC) LUN	SnapCenterのGUIまたはPowerShellコマンドレット	仮想ファイバチャネル スイッチで接続された仮想FC (vFC) LUNのプロビジョニングには、Hyper-V Managerを使用する必要があります。  Hyper-Vのパススルーディスク、およびNetAppストレージでプロビジョニングされたVHD (VHDX) でのデータベースのバックアップはサポートされません。
Hyper-V VM	iSCSIイニシエータでゲスト システムに直接接続されたiSCSI LUN	SnapCenterのGUIまたはPowerShellコマンドレット	 Hyper-Vのパススルーディスク、およびNetAppストレージでプロビジョニングされたVHD (VHDX) でのデータベースのバックアップはサポートされません。

Exchange プラグインに必要な最小ONTAP権限

必要な最小ONTAP権限は、データ保護に使用するSnapCenterプラグインによって異なります。

- 全アクセス コマンド: ONTAP 9.12.1 以降に必要な最小限の権限

- event generate-autosupport-log
- job history show
- job stop
- lun
- lun create
- lun create
- lun create
- lun delete
- lun igroup add
- lun igroup create
- lun igroup delete
- lun igroup rename
- lun igroup rename
- lun igroup show
- lun mapping add-reporting-nodes
- lun mapping create
- lun mapping delete
- lun mapping remove-reporting-nodes
- lun mapping show
- lun modify
- lun move-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- lun resize
- lun serial
- lun show
- snapmirror policy add-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- snapmirror restore
- snapmirror show
- snapmirror show-history
- snapmirror update
- snapmirror update-ls-set
- snapmirror list-destinations

- version
- volume clone create
- volume clone show
- volume clone split start
- volume clone split stop
- volume create
- volume destroy
- volume file clone create
- volume file show-disk-usage
- volume offline
- volume online
- volume modify
- volume qtree create
- volume qtree delete
- volume qtree modify
- volume qtree show
- volume restrict
- volume show
- volume snapshot create
- volume snapshot delete
- volume snapshot modify
- volume snapshot modify-snaplock-expiry-time
- volume snapshot rename
- volume snapshot restore
- volume snapshot restore-file
- volume snapshot show
- volume unmount
- vservers cifs
- vservers cifs share create
- vservers cifs share delete
- vservers cifs shadowcopy show
- vservers cifs share show
- vservers cifs show
- vservers export-policy
- vservers export-policy create
- vservers export-policy delete
- vservers export-policy rule create

- vservers export-policy rule show
- vservers export-policy show
- vservers iscsi
- vservers iscsi connection show
- vservers show
- 読み取り専用コマンド: ONTAP 8.3.0以降に必要な最小限の権限
 - ネットワークインターフェース
 - network interface show
 - SVM

SnapMirrorレプリケーションとSnapVaultレプリケーションのためのストレージ システムの準備

SnapCenterプラグインと一緒にONTAP SnapMirrorテクノロジーを使用すると、バックアップセットのミラー コピーを別のボリュームに作成できます。また、ONTAP SnapVaultを使用すれば、標準への準拠やその他のガバナンスを目的としたディスクツーディスクのバックアップ レプリケーションを実行できます。これらのタスクを実行する前に、ソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenterは、Snapshot処理の完了後に、SnapMirrorとSnapVaultに対する更新を実行します。SnapMirror更新とSnapVault更新は、SnapCenterジョブの一部として実行されるため、ONTAPスケジュールを別途作成しないでください。



NetApp SnapManager製品からSnapCenterに移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリ ストレージ（ソース ボリューム）上のデータがセカンダリ ストレージ（デスティネーション ボリューム）にレプリケートされます。この関係を初期化すると、ソース ボリュームで参照されるデータ ブロックがデスティネーション ボリュームに転送されます。



SnapCenter は、 SnapMirrorとSnapVaultボリューム間のカスケード関係をサポートしていません (* プライマリ * > ミラー > ボールト)。ファンアウト関係を使用する必要があります。

SnapCenterは、バージョンに依存しないSnapMirror関係の管理をサポートしています。バージョンに依存しないSnapMirror関係とその設定方法の詳細については、["ONTAPのドキュメント"](#)。

Exchange Serverリソースのバックアップ戦略の定義

バックアップ ジョブを作成する前にバックアップ戦略を定義しておく、データベースの正常なリストアに必要なバックアップを確実に作成できます。バックアップ戦略の大部分は、サービス レベル アグリーメント（SLA）、目標復旧時間（RTO）、および目標復旧時点（RPO）によって決まります。

SLAは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォー

マンスなど）への対応を定義したものです。RTOは、サービスの停止からビジネス プロセスの復旧までに必要となる時間です。RPOは、障害発生後に通常処理を再開するためにバックアップ ストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA、RTO、およびRPOは、バックアップ戦略に関与します。

Exchangeデータベースでサポートされるバックアップ タイプ

SnapCenterを使用してExchangeメールボックスをバックアップするには、データベースやデータベース可用性グループ（DAG）などのリソース タイプを選択する必要があります。Snapshotテクノロジーを通じて、リソースが配置されているボリュームのオンラインの読み取り専用コピーが作成されます。

バックアップ タイプ	説明
フル / ログ バックアップ	データベースと、切り捨てられたログを含むすべてのトランザクション ログがバックアップされます。 フル バックアップが完了すると、Exchange Serverにより、データベースにコミット済みのトランザクション ログが切り捨てられます。 通常はこのオプションを選択します。ただし、バックアップ時間が短い場合は、フル バックアップでトランザクション ログ バックアップを実行しないように選択することもできます。
フル バックアップ	データベースとトランザクション ログがバックアップされます。 切り捨てられたトランザクション ログはバックアップされません。
ログ バックアップ	すべてのトランザクション ログがバックアップされます。 データベースにコミット済みの切り捨てられたログはバックアップされません。フル データベース バックアップの合間にトランザクション ログを頻繁にバックアップするスケジュールを設定すると、リカバリ ポイントをより細かく選択できます。

データベース プラグインのバックアップ スケジュール

バックアップ頻度（スケジュール タイプ）はポリシーで指定され、バックアップ スケジュールはリソース グループの設定で指定されます。バックアップの頻度またはスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率とデータの重要性です。使用頻度の高いリソースは1時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは1日に1回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービス レベル アグリーメント（SLA）、目標復旧時点（RPO）などがあります。

SLAは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。RPOは、障害発生後に通常処理を再開するためにバックアップ ストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLAとRPOは

データ保護戦略に関わる要件です。

使用頻度の高いリソースであっても、フル バックアップは1日に1～2回で十分です。たとえば、定期的なトランザクション ログ バックアップを実行すれば、必要なバックアップが作成されます。データベースを頻繁にバックアップするほど、SnapCenterが復元時に使用するトランザクション ログが少なくなり、復元操作が高速化されます。

バックアップ スケジュールには、次の2つの要素があります。

- バックアップ頻度

バックアップ頻度 (バックアップを実行する頻度) は、一部のプラグインでは スケジュール タイプ と呼ばれ、ポリシー構成の一部です。ポリシーでは、バックアップ頻度として、毎時、毎日、毎週、または毎月を選択できます。頻度を選択しなかった場合は、オンデマンドのみのポリシーが作成されます。設定 > ポリシー をクリックすると、ポリシーにアクセスできます。

- バックアップ スケジュール

バックアップ スケジュール (バックアップが実行される日時) は、リソース グループ設定の一部です。たとえば、週次バックアップのポリシーが構成されたリソース グループがある場合は、毎週木曜日の午後 10 時にバックアップするようにスケジュールを構成できます。リソース > リソース グループ をクリックすると、リソース グループのスケジュールにアクセスできます。

データベースに必要なバックアップ ジョブの数

必要なバックアップ ジョブの数を左右する要因としては、リソースのサイズ、使用中のボリュームの数、リソースの変更率、サービス レベル アグリーメント (SLA) などがあります。

バックアップの命名規則

Snapshotのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則ではSnapshot名にタイムスタンプが追加されるので、コピーが作成されたタイミングを特定できます。

Snapshotでは、次のデフォルトの命名規則が使用されます。

```
resourcegroupname_hostname_timestamp
```

バックアップ リソース グループには、次の例のように論理的な名前を付ける必要があります。

```
dtst1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- *dtst1* はリソース グループ名です。
- *mach1x88* はホスト名です。
- *03-12-2015_23.17.26* は日付とタイムスタンプです。

または、[スナップショット コピーにカスタム名形式を使用する] を選択して、リソースまたはリソース グループを保護しながらスナップショット名の形式を指定することもできます。たとえ

ば、customtext_resourcegroup_policy_hostnameやresourcegroup_hostnameなどの形式です。デフォルトでは、Snapshot名にタイムスタンプのサフィックスが追加されます。

バックアップ保持オプション

バックアップ コピーを保持する日数を選択するか、または保持するバックアップ コピーの数（ONTAPでは最大255個のコピー）を指定することができます。たとえば、組織の必要に応じて、10日分のバックアップ コピーや130個のバックアップ コピーを保持できます。

ポリシーを作成する際に、バックアップ タイプおよびスケジュール タイプの保持オプションを指定できます。

SnapMirrorレプリケーションを設定すると、デスティネーション ボリュームに保持ポリシーがミラーリングされます。

SnapCenter は、スケジュール タイプに一致する保持ラベルを持つ保持されたバックアップを削除します。リソースまたはリソース グループに対してスケジュール タイプが変更されると、古いスケジュール タイプ ラベルのバックアップがシステムに残ることがあります。



バックアップ コピーを長期にわたって保持する場合は、SnapVaultバックアップを使用する必要があります。

Exchange Serverのソース ストレージ ボリュームにトランザクション ログ バックアップを保持する期間

SnapCenter Plug-in for Microsoft Exchange Serverでは、最新の状態へのリストア処理を実行するために、トランザクション ログ バックアップが必要です。この場合、2つのフル バックアップの間の任意の時点の状態にデータベースがリストアされます。

たとえば、Plug-in for Exchange が午前 8 時に完全バックアップとトランザクション ログ バックアップを実行し、午後 5 時にもう一度完全バックアップとトランザクション ログ バックアップを実行した場合、最新のトランザクション ログ バックアップを使用して、午前 8 時から午後 5 時までの任意の時点にデータベースを復元できます。トランザクション ログが使用できない場合、Plug-in for Exchange は、Plug-in for Exchange が完全バックアップを完了した時点でデータベースを復元するポイントインタイム リストア操作のみを実行できます。

通常、最新の状態へのリストア処理に必要なのは1～2日分のみです。デフォルトでは、SnapCenterの保持期間は最短の2日間です。

Exchangeデータベースのリストア戦略の定義

Exchange Serverのリストア戦略を定義しておくと、その定義に従ってデータベースを実行することができます。

Exchange Serverでのリストア処理のソース

プライマリ ストレージにあるバックアップ コピーからExchange Serverデータベースをリストアすることができます。

データベースはプライマリ ストレージからのみリストアできます。

Exchange Serverでサポートされるリストア処理のタイプ

SnapCenterを使用して、Exchangeのリソースに対してさまざまなタイプのリストア処理を実行できます。

- 最新の状態へのリストア
- 過去のある時点（ポイントインタイム）へのリストア

最新の状態へのリストア

最新の状態へのリストア処理では、障害発生時点までデータベースがリカバリされます。SnapCenterでは、この処理が次の順序で実行されます。

1. 選択したフル データベース バックアップからデータベースがリストアされます。
2. バックアップされたすべてのトランザクション ログと、最新のバックアップ以降に作成された新しいログが適用されます。

トランザクション ログは再生されて選択したすべてのデータベースに適用されます。

リストアの完了後、Exchangeにより新しいログ チェーンが作成されます。

ベスト プラクティス: 復元が完了したら、新しい完全バックアップとログ バックアップを実行することをお勧めします。

最新の状態へのリストア処理を実行するには、連続したトランザクション ログ セットが必要です。

最新の状態へのリストアを実行すると、リストアに使用したバックアップは、ポイントインタイム リストア処理にしか使用できなくなります。

すべてのバックアップに最新の状態へのリストア機能を使用する必要がある場合は、バックアップ ポリシーを使用してシステムのトランザクション ログ バックアップ保持を設定できます。

過去のある時点（ポイントインタイム）へのリストア

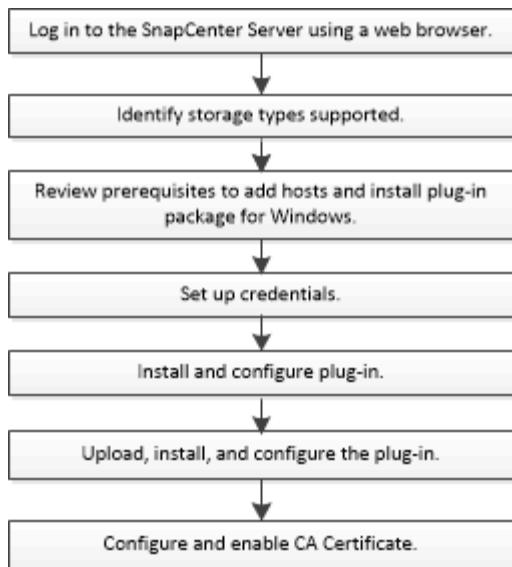
ポイントインタイム リストア処理では、データベースが過去の特定の時点にリストアされます。ポイントインタイム リストア処理は次の状況で発生します。

- バックアップ トランザクション ログの所定の時点までデータベースがリストアされた。
- データベースがリストアされ、一部のバックアップ トランザクション ログだけが適用された。

SnapCenter Plug-in for Microsoft Exchange Serverのインストール

SnapCenter Plug-in for Microsoft Exchange Serverのインストール ワークフロー

Exchangeデータベースを保護する場合は、SnapCenter Plug-in for Microsoft Exchange Serverをインストールしてセットアップする必要があります。



ホストを追加して**SnapCenter Plug-in for Microsoft Exchange Server**をインストールするための前提条件

ホストを追加してプラグイン パッケージをインストールする前に、すべての要件を満たしておく必要があります。

- iSCSIを使用している場合は、iSCSIサービスが実行されている必要があります。
- ローカル管理者権限があり、リモート ホストに対してローカル ログインのアクセス許可があるドメイン ユーザーが必要です。
- スタンドアロン構成およびデータベース可用性グループ構成にMicrosoft Exchange Server 2013、2016、または2019を使用している必要があります。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザーがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。
- SnapCenterでクラスタ ノードを管理する場合は、クラスタ内のすべてのノードに対する管理者権限があるユーザーが必要です。
- Exchange Serverの管理権限があるユーザーが必要です。
- SnapManager for Microsoft Exchange ServerとSnapDrive for Windowsがすでにインストールされている場合は、SnapCenterを使用してデータを確実に保護するために、同じExchange ServerにPlug-in for Exchangeをインストールする前にSnapDrive for Windowsが使用するVSSハードウェア プロバイダの登録を解除しておく必要があります。
- SnapManager for Microsoft Exchange ServerとPlug-in for Exchangeが同じサーバにインストールされている場合は、SnapManager for Microsoft Exchange Serverで作成したすべてのスケジュールをWindowsスケジューラで中断または削除する必要があります。
- サーバからホストを完全修飾ドメイン名 (FQDN) に解決できる必要があります。ホスト ファイルが解決可能になるように変更され、ホスト ファイルで短縮名と FQDN の両方が指定されている場合は、SnapCenterホスト ファイルに次の形式でエントリを作成します: `<ip_address> <host_fqdn> <host_name>`。
- 次のポートがファイアウォールでブロックされていないことを確認します。ブロックされていると、ホストの追加処理に失敗します。この問題を解決するには、動的ポート範囲を設定する必要があります。詳細については、以下を参照してください。 ["Microsoftのドキュメント"](#)。

- Windows 2016とExchange 2016のポート範囲は50,000～51,000です。
- Windows Server 2012 R2とExchange 2013のポート範囲は6,000～6,500です。
- Windows 2019のポート範囲は49,152～65,536です。



ポート範囲を特定するには、次のコマンドを実行します。

- netsh int ipv4 show dynamicport tcp
- netsh int ipv4 show dynamicport udp
- netsh int ipv6 show dynamicport tcp
- netsh int ipv6 show dynamicport udp

SnapCenter Plug-ins Package for Windowsをインストールするホストの要件

SnapCenter Plug-ins Package for Windowsをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	Microsoft Windows サポートされているバージョンに関する最新情報については、" NetApp Interoperability Matrix Tool "。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	5 GB 十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。

項目	要件
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK Java 11 Oracle Java および OpenJDK は、SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp対応プラグイン、および Windows ホストにインストールできるその他のカスタム アプリケーションにのみ必要です。 サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。

必要とされる**Exchange Server**の権限

SnapCenterでExchange ServerまたはDAGを追加し、SnapCenter Plug-in for Microsoft Exchange ServerをホストまたはDAGにインストールできるようにするには、最小限の権限とアクセス許可を持つユーザのクレデンシャルを使用してSnapCenterを設定する必要があります。

ドメイン ユーザには、ローカル管理者権限、リモートExchangeホストに対するローカル ログイン権限、およびDAG内のすべてのノードに対する管理権限が必要です。ドメイン ユーザに必要な最小権限は次のとおりです。

- Add-MailboxDatabaseCopy
- Dismount-Database
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- Move-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:\$true
- Mount-Database
- New-MailboxDatabase
- New-PublicFolderDatabase
- Remove-MailboxDatabase
- Remove-MailboxDatabaseCopy

- Remove-PublicFolderDatabase
- Resume-MailboxDatabaseCopy
- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore:\$true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

SnapCenter Plug-ins Package for Windowsをインストールするホストの要件

SnapCenter Plug-ins Package for Windowsをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	Microsoft Windows サポートされているバージョンに関する最新情報については、" NetApp Interoperability Matrix Tool "。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	5 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。

項目	要件
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK Java 11 Oracle Java および OpenJDK は、SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp対応プラグイン、および Windows ホストにインストールできるその他のカスタム アプリケーションにのみ必要です。 サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。

SnapCenter Plug-in for Windowsのクレデンシャルの設定

SnapCenterは、クレデンシャルを使用してSnapCenterの処理を実行するユーザを認証します。プラグイン パッケージのインストールに使用するクレデンシャルと、データベースでのデータ保護処理に使用するクレデンシャルをそれぞれ作成する必要があります。

タスク概要

Windowsホストにプラグインをインストールするには、クレデンシャルを設定する必要があります。Windowsのクレデンシャルは、ホストを導入してプラグインをインストールしたあとに作成することも可能ですが、SVMを追加したあと、ホストの導入とプラグインのインストールを開始する前に作成することを推奨します。

このクレデンシャルには、管理者権限（リモート ホストに対する管理者権限を含む）を設定します。

個々のリソース グループのクレデンシャルを設定する場合で、ユーザ名に完全なadmin権限が割り当てられていない場合は、少なくともリソース グループとバックアップの権限を割り当てる必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[資格情報]をクリックします。
3. *新規*をクリックします。

[Credential]ウィンドウが表示されます。

4. [Credential]ページで次の操作を実行します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。

フィールド	操作
ユーザー名	認証に使用するユーザ名を入力します。 - ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者またはSnapCenterプラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。ユーザ名フィールドの有効な形式は次のとおりです。 ◦ NetBIOS\UserName ◦ Domain FQDN\UserName - ローカル管理者（ワークグループの場合のみ） ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。ユーザー名フィールドの有効な形式は次のとおりです。 UserName
パスワード	認証に使用するパスワードを入力します。
認証	認証モードとして[Windows]を選択します。

5. [OK]をクリックします。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、作成したグループ管理サービス アカウント（gMSA）を通じて、管理対象ドメイン アカウントからサービス アカウントのパスワードを自動管理できます。

開始する前に

- Windows Server 2016以降のドメイン コントローラが必要です。
- ドメインのメンバーであるWindows Server 2016以降のホストが必要です。

手順

- KDSルート キーを作成し、gMSA内のオブジェクトごとに一意のパスワードを生成します。
- 各ドメインについて、Windowsドメインコントローラから次のコマンドを実行します: Add-KDSRootKey -Effectivelmmmediately

3. gMSAを作成して設定します。

- a. 次の形式でユーザ グループ アカウントを作成します。

```
domainName\accountName$  
.. コンピュータ オブジェクトをグループに追加します。  
.. 作成したユーザ グループを使用してgMSAを作成します。
```

次に例を示します。

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 走る `Get-ADServiceAccount` サービス アカウントを確認するコマンド。
```

4. ホストでgMSAを設定します。

- a. gMSAアカウントを使用するホストで、Windows PowerShell用のActive Directoryモジュールを有効にします。

これを行うには、PowerShellから次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart	Needed	Exit Code	Feature Result
-----	-----	-----	-----	-----
True	No		Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. ホストを再起動します。
- b. PowerShell コマンド プロンプトから次のコマンドを実行して、ホストに gMSA をインストールします。 `Install-AdServiceAccount <gMSA>`
- c. 次のコマンドを実行して、gMSA アカウントを確認します。 `Test-AdServiceAccount <gMSA>`

5. ホスト上の設定済みgMSAに管理者権限を割り当てます。
6. SnapCenter Serverで設定済みのgMSAアカウントを指定してWindowsホストを追加します。

SnapCenter Serverにより、選択したプラグインがホストにインストールされ、プラグインのインストール時には指定したgMSAがサービスのログオン アカウントとして使用されます。

ホストの追加とPlug-in for Exchangeのインストール

SnapCenterの[Add Host]ページを使用して、Windowsホストを追加できます。Plug-in for Exchangeは、指定したホストに自動的にインストールされます。これは推奨されるプラグインのインストール方法です。ホストの追加とプラグインのインストールは、ホストごとまたはクラスタごとに実行できます。

開始する前に

- SnapCenter Serverホストのオペレーティング システムがWindows 2019で、プラグイン ホストのオペレーティング システムがWindows 2022の場合は、次の手順を実行する必要があります。
 - Windows Server 2019 (OSビルド17763.5936) 以降にアップグレードする
 - Windows Server 2022 (OSビルド20348.2402) 以降にアップグレードする
- この処理は、SnapCenter Adminなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。
- メッセージ キュー サービスが実行されている必要があります。
- グループ管理サービス アカウント (gMSA) を使用する場合は、管理者権限でgMSAを設定する必要があります。詳細については、"[Windows Server 2016 以降で Microsoft Exchange Server のグループ管理サービス アカウントを構成する](#)"。

タスク概要

- SnapCenter Serverをプラグイン ホストとして別のSnapCenter Serverに追加することはできません。
- ホストの追加とプラグイン パッケージのインストールは、ホストごとまたはクラスタごとに実行できます。
- ExchangeノードがDAGの一部である場合、SnapCenter Serverにノードを1つだけ追加することはできません。
- クラスタ (Exchange DAG) にプラグインをインストールする場合は、NetApp LUN上にデータベースのないノードがあったとしても、クラスタのすべてのノードにプラグインがインストールされます。

SnapCenter 4.6以降では、SCEがマルチテナンシー対応になったので、次の方法でホストを追加できます。

ホストの追加処理	4.5以前	4.6以降
クロス ドメインまたは別のドメインのIPレスDAGを追加	サポート対象外	サポート
同一ドメインまたはクロス ドメインに存在する、一意の名前を持つ複数のIP DAGを追加	サポート	サポート

ホストの追加処理	4.5以前	4.6以降
クロス ドメインで同一のホスト名やDB名を持つ複数のIP DAGまたはIPレスDAGを追加	サポート対象外	サポート
クロス ドメインで同一の名前を持つ複数のIP DAGまたはIPレスDAGを追加	サポート対象外	サポート
クロス ドメインで同一の名前を持つ複数のスタンドアロン ホストを追加	サポート対象外	サポート

Plug-in for ExchangeはSnapCenter Plug-ins Package for Windowsに依存するため、同一のバージョンである必要があります。Plug-in for Exchangeのインストール時には、SnapCenter Plug-ins Package for Windowsがデフォルトで選択され、VSSハードウェア プロバイダとともにインストールされます。

SnapManager for Microsoft Exchange ServerとSnapDrive for WindowsがすでにインストールされているExchange ServerにPlug-in for Exchangeをインストールする場合は、SnapDrive for Windowsで使用されているVSSハードウェア プロバイダは、Plug-in for ExchangeおよびSnapCenter Plug-ins Package for WindowsとともにインストールされるVSSハードウェア プロバイダと互換性がないため、登録を解除する必要があります。詳細については、以下を参照してください。"[Data ONTAP VSSハードウェアプロバイダを手動で登録する方法](#)"。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. 上部で*管理対象ホスト*が選択されていることを確認します。
3. *[追加]*をクリックします。
4. [Hosts]ページで次の操作を実行します。

フィールド	操作
ホストタイプ	ホストタイプとして*Windows*を選択します。 SnapCenter Serverがホストを追加し、Plug-in for WindowsとPlug-in for Exchangeをホストにインストールします（プラグインがまだインストールされていない場合）。 Plug-in for WindowsとPlug-in for Exchangeのバージョンは同じである必要があります。異なるバージョンのPlug-in for Windowsが以前にインストールされていた場合は、SnapCenterのインストール時にバージョンが更新されます。

フィールド	操作
ホスト名	ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。 SnapCenterが機能するためには、DNSが適切に設定されている必要があります。したがって、ベストプラクティスはFQDNを入力することです。 信頼されないドメイン ホストのIPアドレスがサポートされるのは、そのIPアドレスがFQDNに解決される場合のみです。 SnapCenterを使用してホストを追加する際、ホストがサブドメインの一部である場合は、FQDNを指定する必要があります。 次のいずれかのIPアドレスまたはFQDNを入力できます。 • スタンドアロン ホスト • Exchange DAG Exchange DAGの場合は、次の操作を実行できます。 ◦ DAG名、DAGのIPアドレス、ノード名、またはノードIPアドレスを指定してDAGを追加する。 ◦ いずれかのDAGクラスター ノードのIPアドレスまたはFQDNを指定して、IPレスDAGクラスターを追加する。 ◦ 同一ドメインまたは別のドメインに存在するIPレスDAGを追加する。同じ名前異なるドメインの複数のIP DAGまたはIPレスDAGを追加することもできます。  スタンドアロン ホストまたはExchange DAG（クロス ドメインまたは同一ドメイン）の場合は、ホストまたはDAGのFQDNかIPアドレスを指定することを推奨します。

フィールド	操作
Credentials	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモート ホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 指定したクレデンシャル名にカーソルを合わせると、クレデンシャルの詳細を確認できます。  クレデンシャルの認証モードは、ホスト追加ウィザードで指定するホストタイプによって決まります。

5. [Select Plug-ins to Install]セクションで、インストールするプラグインを選択します。

Plug-in for Exchangeを選択すると、SnapCenter Plug-in for Microsoft SQL Serverの選択が自動的に解除されます。Microsoftでは、Exchangeで必要とされるメモリ使用量やその他のリソース使用量を考慮して、SQL ServerとExchange Serverを同じシステムにインストールしないことを推奨しています。

6. (オプション) [その他のオプション] をクリックします。

フィールド	操作
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。 デフォルトのポート番号は8145です。SnapCenter Serverがカスタム ポートにインストールされている場合は、そのポート番号がデフォルト ポートとして表示されます。  プラグインを手動でインストールしてカスタム ポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理が失敗します。
Installation Path	デフォルトのパスは C:\Program Files\NetApp\SnapCenter。 必要に応じて変更できます。
Add all hosts in the DAG	DAGを追加する場合は、このチェック ボックスをオンにします。

フィールド	操作
Skip preinstall checks	プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスをオンにします。
Use group Managed Service Account (gMSA) to run the plug-in services	グループ管理サービス アカウント (gMSA) を使用してプラグイン サービスを実行する場合は、このチェック ボックスをオンにします。 gMSA 名を次の形式で指定します: <code>domainName\accountName\$</code>。  gMSAは、SnapCenter Plug-in for Windowsサービスのログオン サービス アカウントとしてのみ使用されます。

7. *送信*をクリックします。

[Skip prechecks]チェック ボックスをオフにしていると、ホストがプラグインをインストールするための要件を満たしているかどうかを確認するための検証が行われます。最小要件を満たしていない場合は、該当するエラーまたは警告メッセージが表示されます。

エラーがディスク容量またはRAMに関連している場合は、次の場所にあるweb.configファイルを更新できます。`C:\Program Files\NetApp\SnapCenter`デフォルト値を変更する WebApp。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。



HAのセットアップでweb.configファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. インストールの進捗状況を監視します。

NET TCP通信用のカスタム ポートの設定

デフォルトでは、SnapCenter 6.0 リリース以降、Windows 用のSnapCenterプラグインは、NET TCP 通信にポート 909 を使用します。ポート909が使用中の場合は、NET TCP通信用に別のポートを設定できます。

手順

1. `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vsproviders\navssprv.exe.config` にある `NetTCPPort` キーの値を必要なポート番号に変更します。
`<add key="NetTCPPort" value="new_port_number" />`
2. `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\SnapDriveService.dll.config` にある `NetTCPPort` キーの値を必要なポート番号に変更します。
`<add key="NetTCPPort" value="new_port_number" />`
3. 以下のコマンドを実行して、*Data ONTAP VSS Hardware Provider* サービスの登録を解除します。
`"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft`


```
Windows\navssprv.exe" -r service -u
```

services.msc のサービス リストにサービスが表示されていないことを確認します。

4. 以下のコマンドを実行して、*Data ONTAP VSS Hardware Provider* サービスを登録します。
"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"

services.msc のサービス リストにサービスが表示されているかどうかを確認します。

5. *Plug-in for Windows* サービスを再起動します。

PowerShellコマンドレットを使用したSnapCenter ServerホストからのPlug-in for Exchangeのインストール

Plug-in for ExchangeはSnapCenter GUIからインストールする必要があります。GUIを使用しない場合は、SnapCenter Serverホストまたはリモート ホストでPowerShellコマンドレットを使用できます。

開始する前に

- SnapCenter Serverがインストールおよび設定されている必要があります。
- ホストのローカル管理者または管理権限を持つユーザである必要があります。
- この処理は、SnapCenter Adminなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。
- Plug-in for Exchangeをインストールする前に、インストール要件とサポートされる構成のタイプを確認しておく必要があります。
- Plug-in for ExchangeをインストールするホストとしてWindowsホストを使用する必要があります。

手順

1. SnapCenter Server ホストで、*Open-SmConnection* コマンドレットを使用してセッションを確立し、資格情報を入力します。
2. 必要なパラメータを指定した *Add-SmHost* コマンドレットを使用して、Exchange 用プラグインをインストールするホストを追加します。

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

ホストとしてスタンドアロン ホストまたはDAGを指定できます。DAG を指定する場合、*-IsDAG* パラメータは必須です。

3. 必要なパラメータを指定した *Install-SmHostPackage* コマンドレットを使用して、Exchange 用プラグインをインストールします。

このコマンドを実行すると、指定したホストにPlug-in for Exchangeがインストールされて、SnapCenterに登録されます。

コマンドラインからの**SnapCenter Plug-in for Exchange**のサイレント インストール

Plug-in for ExchangeはSnapCenterユーザ インターフェイス内からインストールする必要があります。ただし、何らかの理由でインストールできない場合は、Windowsのコマンドラインから、Plug-in for Exchangeのインストール プログラムをサイレント モードで自動的に実行できます。

開始する前に

- Microsoft Exchange Serverリソースをバックアップしておく必要があります。
- SnapCenterプラグイン パッケージをインストールしておく必要があります。
- インストール前に、以前のリリースのSnapCenter Plug-in for Microsoft SQL Serverを削除する必要があります。

詳細については、以下を参照してください。 ["SnapCenterプラグインをプラグインホストから手動で直接インストールする方法"](#)。

手順

1. プラグイン ホストに `C:\temp` フォルダが存在し、ログインしたユーザーがそのフォルダにフル アクセス権を持っているかどうかを検証します。
2. `C:\ProgramData\NetApp\SnapCenter\Package` リポジトリから Microsoft Windows 用のSnapCenterプラグインをダウンロードします。

このパスには、SnapCenter Serverがインストールされているホストからアクセスできます。

3. プラグインをインストールするホストにインストール ファイルをコピーします。
4. ローカル ホストのWindowsコマンド プロンプトで、プラグインのインストール ファイルを保存したディレクトリに移動します。
5. 次のコマンドを入力してプラグインをインストールします。

```
snapcenter_windows_host_plugin.exe"/silent /debuglog"<デバッグログパス>" /log"<ログパス>"  
BI_SNAPCENTER_PORT=<番号> SUITE_INSTALLDIR=<インストールディレクトリパス>"  
BI_SERVICEACCOUNT=<ドメイン\管理者> BI_SERVICEPWD=<パスワード>  
ISFeatureInstall=HPPW,SCW,SCE
```

例えば：

```
C:\ProgramData\NetApp\SnapCenter\Package Repository\snapcenter_windows_host_plugin.exe"/silent  
/debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\temp" BI_SNAPCENTER_PORT=8145  
SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=HPPW,SCW,SCE
```



Plug-in for Exchangeのインストール時に渡されるすべてのパラメータでは、大文字と小文字が区別されます。

変数には次の値を入力します。

変数	Value
/debuglog"<デバッグログパス>	インストーラのログ ファイルの名前と場所を次のように指定します。 <i>Setup.exe /debuglog"C:\PathToLog\setupexe.log</i>
BI_SNAPCENTER_PORT	SnapCenterがSMCoreと通信するポートを指定します。
SUITE_INSTALLDIR	ホストのプラグイン パッケージのインストール ディレクトリを指定します。
BI_SERVICEACCOUNT	SnapCenter Plug-in for Microsoft WindowsのWebサービス アカウントを指定します。
BI_SERVICEPWD	SnapCenter Plug-in for Microsoft WindowsのWebサービス アカウントのパスワードを指定します。
ISFeatureInstall	SnapCenterでリモート ホストに導入するソリューションを指定します。

- Windows タスク スケジューラ、メインのインストール ログ ファイル *C:\Installdebug.log*、および *C:\Temp* 内の追加のインストール ファイルを監視します。
- %temp%* ディレクトリを監視して、*msiexe.exe* インストーラーがエラーなしでソフトウェアをインストールしているかどうかを確認します。



Plug-in for Exchangeをインストールすると、SnapCenter Serverではなくホストにプラグインが登録されます。SnapCenter GUIまたはPowerShellコマンドレットを使用してホストを追加することにより、SnapCenter Serverにプラグインを登録できます。ホストを追加すると、プラグインが自動的に検出されます。

SnapCenterプラグイン パッケージのインストール ステータスの監視

[Jobs]ページを使用して、SnapCenterプラグイン パッケージのインストールの進捗状況を監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-

 警告付きで完了したか、警告のため開始できませんでした

-  キューに登録

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、プラグインのインストール操作のみがリストされるようにリストをフィルタリングするには、次の手順を実行します。
 - a. *フィルター*をクリックします。
 - b. オプション：開始日と終了日を指定します。
 - c. [タイプ] ドロップダウン メニューから、[プラグインのインストール] を選択します。
 - d. [Status]ドロップダウン メニューから、インストールのステータスを選択します。
 - e. *適用*をクリックします。
4. インストール ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

CA証明書の設定

CA証明書CSRファイルの生成

証明書署名要求（CSR）を生成し、生成したCSRを使用して認証局（CA）から取得した証明書をインポートできます。証明書には秘密キーが関連付けられます。

CSRはエンコードされたテキストのブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。

 CA 証明書の RSA キーの長さは最低 3072 ビットである必要があります。

CSRを生成するための情報については、["CA証明書CSRファイルの生成方法"](#)。

 ドメイン (*.domain.company.com) またはシステム (machine1.domain.company.com) の CA 証明書を所有している場合は、CA 証明書 CSR ファイルの生成をスキップできます。SnapCenterを使用して、既存のCA証明書を導入できます。

クラスタ構成の場合、クラスタ名（仮想クラスタFQDN）と、それぞれのホスト名がCA証明書に記載されている必要があります。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。ワイルドカード証明書 (*.domain.company.com) の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenter ServerとWindowsホスト プラグインにCA証明書をインポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
4. コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書 をクリックします。
5. 「信頼されたルート証明機関」フォルダを右クリックし、[すべてのタスク] > [インポート] を選択して、インポート ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*次へ*をクリックします。
インポート ファイル形式	変更せずに、[次へ] をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、[次へ] をクリックします。
証明書のインポート ウィザードの完了	概要を確認し、[完了] をクリックしてインポートを開始します。



インポートする証明書は秘密キーとバンドルされている必要があります (サポートされている形式は **.pfx**、**.p12**、および ***.p7b** です)。

7. 「個人用」フォルダに対して手順5を繰り返します。

CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための16進数の文字列です。サムプリントは、サムプリント アルゴリズムを使用して証明書の内容から計算されます。

手順

1. GUIで次の手順を実行します。
 - a. 証明書をダブルクリックします。
 - b. [証明書] ダイアログボックスで、[詳細] タブをクリックします。
 - c. フィールドのリストをスクロールして、「拇印」をクリックします。
 - d. ボックスから16進数の文字をコピーします。
 - e. 16進数の間のスペースを削除します。

たとえば、拇印が「a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b」の場合、スペース

を削除すると「a909502dd82ae41433e6f83886b00d4277a32a7b」になります。

2. PowerShellで、次の手順を実行します。

- a. 次のコマンドを実行して、インストールされている証明書のサムプリントを表示し、最近インストールされた証明書をサブジェクト名で識別します。

```
Get-ChildItem -Path 証明書:\LocalMachine\My
```

- b. サムプリントをコピーします。

Windowsホスト プラグイン サービスでのCA証明書の設定

インストールされているデジタル証明書をアクティブ化するには、Windowsホスト プラグイン サービスを使用してCA証明書を設定する必要があります。

SnapCenter Serverと、CA証明書がすでに導入されているすべてのプラグイン ホストで、次の手順を実行します。

手順

1. 次のコマンドを実行して、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例えば：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

． 次のコマンドを実行して、新しくインストールした証明書をWindowsホスト プラグイン サービスとバインドします。

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例えば：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

プラグインのCA証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。

あります。プラグインでCA証明書の検証を有効にする必要があります。

開始する前に

- 実行 `Set-SmCertificateSettings` コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- `Get-SmCertificateSettings` を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. プラグイン ホストを1つまたは複数選択します。
4. *その他のオプション* をクリックします。
5. *証明書の検証を有効にする* を選択します。

終了後の操作

[Managed Hosts] タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Serverとプラグイン ホスト間の接続のステータスを示します。

- *  * は、CA 証明書が有効になっていないか、プラグイン ホストに割り当てられていないことを示します。
- *  * は CA 証明書が正常に検証されたことを示します。
- *  * は、CA 証明書を検証できなかったことを示します。
- *  * は接続情報を取得できなかったことを示します。



ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

SnapManager 7.x for ExchangeとSnapCenterの共存の設定

SnapCenter Plug-in for Microsoft Exchange ServerとSnapManager for Microsoft Exchange Serverを共存させるには、SnapManager for Microsoft Exchange Serverがインストールされているのと同じExchange ServerにSnapCenter Plug-in for Microsoft Exchange Serverをインストールし、SnapManager for Exchangeのスケジュールを無効にして、SnapCenter Plug-in for Microsoft Exchange Serverで新しいスケジュールとバックアップを設定する必要があります。

開始する前に

- SnapManager for Microsoft Exchange ServerとSnapDrive for Windowsがすでにインストールされていて、SnapManager for Microsoft Exchange ServerのバックアップがシステムのSnapInfoディレクトリに保存されている必要があります。
- SnapManager for Microsoft Exchange Serverで作成した不要なバックアップを削除または再利用しておく必要があります。

- SnapManager for Microsoft Exchange Serverで作成したすべてのスケジュールを、Windowsスケジューラで一時停止または削除しておく必要があります。
- SnapCenter Plug-in for Microsoft Exchange ServerとSnapManager for Microsoft Exchange Serverは同じExchange Serverに共存させることができますが、既存のSnapManager for Microsoft Exchange Server環境をSnapCenterにアップグレードすることはできません。

SnapCenterにはアップグレード オプションが用意されていません。

- SnapCenterでは、SnapManager for Microsoft Exchange ServerのバックアップからのExchangeデータベースのリストアがサポートされていません。

SnapCenter Plug-in for Microsoft Exchange Serverのインストール後にSnapManager for Microsoft Exchange Serverをアンインストールせずに、SnapManager for Microsoft Exchange Serverのバックアップをあとからリストアする場合は、追加の手順を実行する必要があります。

手順

1. すべての DAG ノードで PowerShell を使用して、SnapDrive for Windows VSS ハードウェア プロバイダーが登録されているかどうかを確認します: *vssadmin list providers*

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
Version: 7. 1. 4. 6845
```

2. SnapDriveディレクトリから、SnapDrive for WindowsからVSSハードウェアプロバイダーの登録を解除します: *navssprv.exe -r service -u*
3. VSS ハードウェア プロバイダーが削除されたことを確認します: *vssadmin list providers*
4. ExchangeホストをSnapCenterに追加して、SnapCenter Plug-in for Microsoft WindowsとSnapCenter Plug-in for Microsoft Exchange Serverをインストールします。
5. すべてのDAGノードのSnapCenter Plug-in for Microsoft Windowsディレクトリから、VSSハードウェアプロバイダーが登録されていることを確認します: *vssadmin list providers*


```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
Version: 7. 0. 0. 5561
```

6. SnapManager for Microsoft Exchange Serverのバックアップ スケジュールを停止します。
7. SnapCenter GUIを使用して、オンデマンド バックアップの作成、スケジュール済みバックアップの設定、保持設定の指定を行います。
8. SnapManager for Microsoft Exchange Serverをアンインストールします。

SnapManager for Microsoft Exchange Serverをすぐにアンインストールせずに、SnapManager for Microsoft Exchange Serverのバックアップをあとからリストアする場合は、次の手順を実行します。

- a. すべての DAG ノードから Microsoft Exchange Server 用SnapCenterプラグインの登録を解除します:
navssprv.exe -r service -u

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
Windows>navssprv.exe -r service -u
```

- b. *C:\Program Files\NetApp\SnapDrive*ディレクトリから、すべての DAG ノードにSnapDrive for Windows を登録します: *navssprv.exe -r service -a hostname\username -p password*

SnapCenter Plug-in for VMware vSphereのインストール

データベースまたはファイルシステムが仮想マシン（VM）に格納されている場合や、VMとデータストアを保護する場合は、SnapCenter Plug-in for VMware vSphere仮想アプライアンスを導入する必要があります。

展開方法については、"[導入プロセスの概要](#)"。

CA証明書を導入する

SnapCenter Plug-in for VMware vSphereで CA 証明書を構成するには、以下を参照してください。"[SSL証明書を作成またはインポートする](#)"。

CRLファイルを設定する

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリでCRLファイルを探します。SnapCenter Plug-in for VMware vSphere のCRL ファイルのデフォルト ディレクトリは */opt/netapp/config/crl* です。

このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

データ保護の準備

バックアップ、クローニング、リストアなどのデータ保護処理を実行する場合は、事前に戦略を定義し、環境をセットアップする必要があります。SnapMirrorテクノロジーとSnapVaultテクノロジーを使用できるようにSnapCenter Serverをセットアップすることもできます。

SnapVaultテクノロジーとSnapMirrorテクノロジーを利用するには、ストレージ デバイス上のソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、初期化する必要があります。この作業を実行するには、NetApp System Managerを使用するか、ストレージ コンソールのコマンドラインを使用します。

詳細情報

["REST APIの使用"](#)

SnapCenter Plug-in for Microsoft Exchange Serverを使用するための前提条件

ユーザがPlug-in for Exchangeを使用するためには、SnapCenter管理者が事前にSnapCenter Serverをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter Serverをインストールして設定します。
- SnapCenterにログインします。
- SnapCenter環境を設定するために、ストレージ システム接続の追加または割り当てを行い、クレデンシヤルを作成します。



SnapCenterでは、別々のクラスタに属している場合でも、複数のSVMに同じ名前を付けることはサポートされません。SnapCenterでサポートするSVMには、すべて一意の名前を付ける必要があります。

- ホストを追加し、SnapCenter Plug-in for Microsoft WindowsとSnapCenter Plug-in for Microsoft Exchange Serverをインストールして、リソースを検出（更新）します。
- SnapCenter Plug-in for Microsoft Windowsを使用して、ホスト側のストレージをプロビジョニングします。
- SnapCenter Serverを使用してVMware RDM LUN上のExchangeデータベースを保護する場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。詳細については、SnapCenter Plug-in for VMware vSphereのドキュメントを参照してください。



VMDKはサポートされません。

- Microsoft Exchangeのツールを使用して、既存のMicrosoft Exchange Serverデータベースをローカル ディスクからサポート対象のストレージに移動します。
- バックアップ レプリケーションが必要である場合は、SnapMirror関係とSnapVault関係をセットアップします。

SnapCenter Plug-in for VMware vSphere 4.1.1のドキュメントには、SnapCenter 4.1.1のユーザ向けに、仮想データベースとファイルシステムの保護に関する情報が記載されています。NetApp Data Broker 1.0および1.0.1のドキュメントには、SnapCenter 4.2.xのユーザ向けに、LinuxベースのNetApp Data Broker仮想アプライアンス（オープン仮想アプライアンス形式）が提供するSnapCenter Plug-in for VMware vSphereを使用した仮想データベースとファイルシステムの保護に関する情報が記載されています。SnapCenter Plug-in for VMware vSphere 4.3のドキュメントには、SnapCenter 4.3.xのユーザ向けに、LinuxベースのSnapCenter Plug-in for VMware vSphere仮想アプライアンス（オープン仮想アプライアンス形式）を使用した仮想データベースとファイルシステムの保護に関する情報が記載されています。

"SnapCenter Plug-in for VMware vSphereのドキュメント"

Exchange Serverの保護におけるソース、リソース グループ、ポリシーの使用方法

SnapCenterを使用する前に、実行するバックアップ、リストア、再シードの各処理に関連する基本的な概念を理解しておくことが役立ちます。ここでは、これらの処理で扱うリソース、リソース グループ、およびポリシーについて説明します。

- リソースとは、通常は、SnapCenterでバックアップするメールボックス データベースまたはMicrosoft Exchangeデータベース可用性グループ（DAG）です。
- SnapCenterのリソース グループは、ホストまたはExchange DAG上のリソースの集まりであり、リソース グループにはDAG全体または個々のデータベースを含めることができます。

リソース グループに対して処理を実行すると、リソース グループに指定したスケジュールに従って、リソース グループに定義されているリソースに対して処理が実行されます。

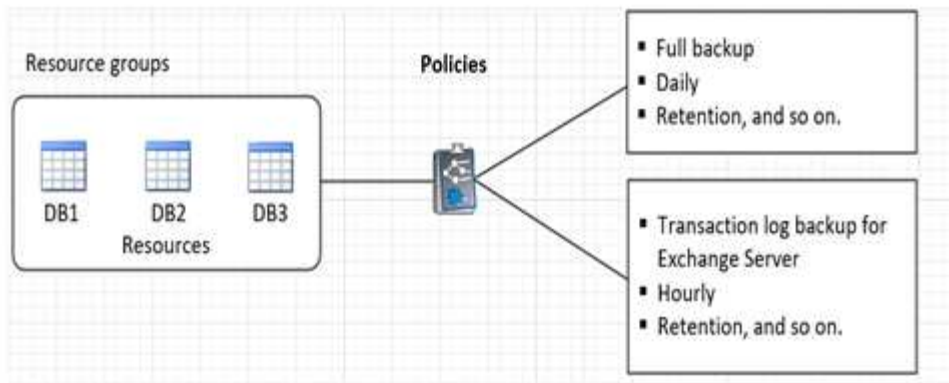
単一のリソースまたはリソース グループをオンデマンドでバックアップすることができます。また、スケジュールされたバックアップを単一リソースおよびリソース グループに対して実行することもできます。

リソース グループは、以前はデータセットと呼ばれていました。

- ポリシーは、バックアップ頻度、コピーの保持、スクリプトといった、データ保護処理の特性を指定するものです。

リソース グループを作成するときに、そのグループに対して1つ以上のポリシーを選択します。オンデマンドで単一リソースのバックアップを実行するときにも、1つ以上のポリシーを選択できます。

リソース グループは、保護する対象と、それを日時でいつ保護するかを定義するものと考えてください。ポリシーとは、それをどのように保護したいかを定義するものと考えてください。たとえば、ホストのすべてのデータベースをバックアップする場合は、ホストのすべてのデータベースを含むリソース グループを作成します。このリソース グループに、日次ポリシーと毎時ポリシーの2つのポリシーを適用します。リソース グループを作成してポリシーを適用する際に、フル バックアップを1日1回実行するようにリソース グループを設定し、別のスケジュールでログ バックアップを1時間おきに実行するように設定します。次の図は、データベースのリソース、リソース グループ、ポリシーの関係を示しています。



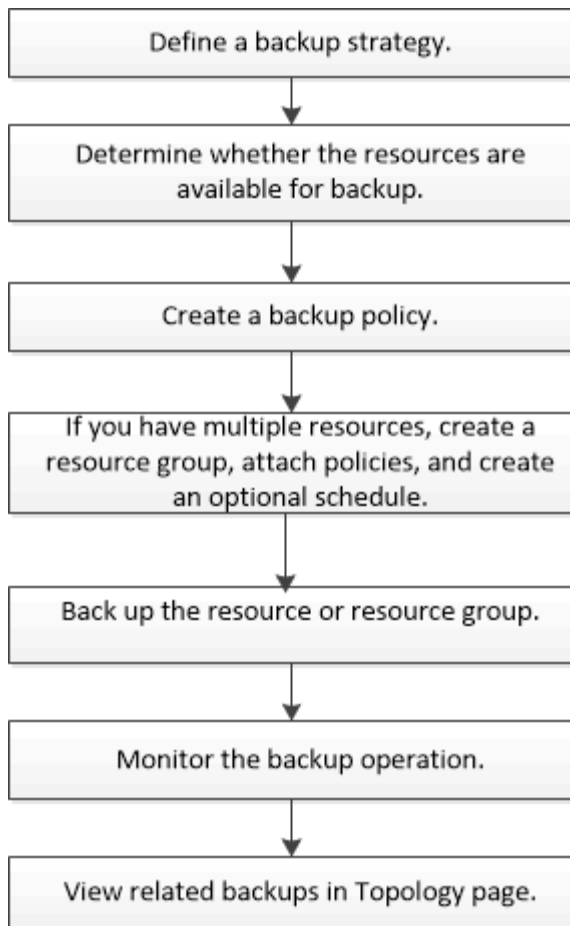
Exchange リソースのバックアップ

バックアップのワークフロー

SnapCenter Plug-in for Microsoft Exchange Serverをインストールした環境では、SnapCenterを使用してExchange リソースをバックアップすることができます。

スケジュールを設定して、複数のサーバで同時に複数のバックアップを実行することができます。同じリソースに対してバックアップ処理とリストア処理を同時に実行することはできません。同じボリューム上でのアクティブ バックアップ コピーとパッシブ バックアップ コピーはサポートされていません。

次のワークフローは、バックアップ処理の実行順序を示しています。



Exchangeのデータベースとバックアップの検証

SnapCenter Plug-in for Microsoft Exchange Serverではバックアップの検証は行われませんが、Exchangeに付属するEseutilツールを使用して、Exchangeのデータベースとバックアップを検証できます。

Microsoft Exchange Eseutilツールは、Exchange Serverに付属するコマンドライン ユーティリティです。このユーティリティを使用すると、整合性チェックを実行して、Exchangeのデータベースとバックアップの整合性を検証できます。

ベスト プラクティス: 少なくとも 2 つのレプリカを持つデータベース可用性グループ (DAG) 構成の一部であるデータベースに対して整合性チェックを実行する必要はありません。

詳細については、"[Microsoft Exchange Server ドキュメント](#)"。

Exchangeのリソースをバックアップに使用できるかどうかの確認

リソースとは、インストールしたプラグインで管理されるデータベースやExchangeデータベース可用性グループのことです。リソースをリソース グループに追加することでデータ保護ジョブを実行できますが、その前に使用可能なリソースを特定しておく必要があります。使用可能なリソースを確認することで、プラグインのインストールが正常に完了したことの確認にもなります。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の作成、クレデンシャルの追加、Plug-in for Exchangeのインストールなどのタスクを完了しておく必要があります。
- Single Mailbox Recoveryソフトウェアの機能を利用するには、Single Mailbox RecoveryソフトウェアがインストールされているExchange Serverにアクティブなデータベースを配置しておく必要があります。
- データベースがVMware RDM LUN上にある場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。その ["SnapCenter Plug-in for VMware vSphereのドキュメント"](#) 詳細情報があります。

タスク概要

- 詳細ページの*全体的なステータス*オプションがバックアップ不可に設定されている場合は、データベースをバックアップできません。次のいずれかに該当する場合、全体的なステータス オプションはバックアップに利用できませんに設定されます。
 - データベースがNetApp LUN上にない。
 - データベースが正常な状態でない。

データベースの状態がマウント、アンマウント、再シード、リカバリ保留中のいずれかのときは、正常な状態ではありません。

- データベース可用性グループ (DAG) がある場合は、DAGからバックアップ ジョブを実行して、グループ内のすべてのデータベースをバックアップできます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、[リソース] ページの左上隅にあるプラグイン ドロップダウン リストから **[Microsoft Exchange Server]** を選択します。
2. [リソース] ページで、[表示] ドロップダウン リストから [データベース]、[データベース可用性グループ]、または [リソース グループ] を選択します。

すべてのデータベースとDAGは、完全修飾ドメイン名 (FQDN) 形式でそれぞれのDAG名やホスト名が表示されるので、データベースが複数あっても識別できます。

クリック  ホスト名と Exchange Server を選択して、リソースをフィルターします。そのあとに  をクリックすると、フィルタ ペインが閉じます。

3. *リソースの更新*をクリックします。

新たに追加、名称変更、削除されたリソースが、SnapCenter Serverのインベントリで更新されます。



SnapCenterの外部でデータベースの名前が変更された場合は、リソースを更新する必要があります。

リソースは、リソース名、データベース可用性グループ名、データベースが現在アクティブなサーバ、コピーがあるサーバ、前回のバックアップ時刻、全体的なステータスなどの情報とともに表示されます。

- データベースが他社ストレージにある場合は、[Overall Status]列に「Not available for backup」と表示されます。

DAG では、アクティブ データベース コピーがNetApp以外のストレージ上にあり、少なくとも 1 つのパッシブ データベース コピーがNetAppストレージ上にある場合、全体的なステータス 列に「保護さ

れていません」と表示されます。

他社ストレージ タイプにあるデータベースには、データ保護処理を実行できません。

- データベースがNetAppストレージ上にあり、保護されていない場合は、[全体的なステータス] 列に [保護されていません] と表示されます。
- データベースがNetAppストレージ システム上にあり、保護されている場合、ユーザー インターフェイスの 全体的なステータス 列に「バックアップは実行されていません」というメッセージが表示されます。
- データベースがNetAppストレージ システム上にあり、保護されており、データベースのバックアップがトリガーされた場合、ユーザー インターフェイスの [全体的なステータス] 列に [バックアップが成功しました] というメッセージが表示されます。

Exchange Serverデータベースのバックアップ ポリシーの作成

SnapCenterを使用してMicrosoft Exchange Serverリソースをバックアップする前に、Exchangeリソースまたはリソース グループのバックアップ ポリシーを作成することができます。また、リソース グループの作成時や単一のリソースのバックアップ時にバックアップ ポリシーを作成することも可能です。

開始する前に

- データ保護戦略を定義しておく必要があります。

詳細については、Exchangeデータベースのデータ保護戦略の定義に関する説明を参照してください。

- SnapCenterのインストール、ホストの追加、リソースの特定、ストレージ システム接続の作成などのタスクを実行して、データ保護の準備をしておく必要があります。
- Exchange Serverリソースを更新（検出）しておく必要があります。
- Snapshotをミラーまたはバックアップにレプリケートするユーザには、SnapCenter管理者がユーザに対してソースとデスティネーションの両方のボリューム用にStorage Virtual Machine（SVM）を割り当てておく必要があります。
- PowerShellスクリプトをプレスクリプトとポストスクリプトで実行したい場合は、``usePowershellProcessforScripts`` パラメータをtrueに設定する ``web.config`` ファイル。

デフォルト値はfalseです。

- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、["SnapMirrorアクティブ同期のオブジェクト数の制限"](#)。

タスク概要

- バックアップ ポリシーとは、バックアップを管理および保持する方法やリソースやリソース グループをバックアップする頻度を定めた一連のルールです。また、スクリプト設定を指定することもできます。ポリシーでオプションを指定しておくことで、別のリソース グループにポリシーを再利用して時間を節約することができます。
- フル バックアップの保持設定は、ポリシーごとに固有です。フル バックアップの保持数が4のポリシーAを使用するデータベースやリソースでは4つのフル バックアップが保持され、同じデータベースやリソースのポリシーBには影響しません。ポリシーBの保持数が3であれば、ポリシーBを使用すると3つのフル バックアップが保持されます。

- ログ バックアップの保持設定はポリシーの違いを超えて影響を及ぼし、データベースやリソースのすべてのログ バックアップに適用されます。したがって、ポリシーBを使用してフル バックアップを実行すると、そのログ保持設定は、同じデータベースやリソースの、ポリシーAで作成されたログ バックアップに影響します。同様に、ポリシーAのログ保持設定は、同じデータベースの、ポリシーBで作成されたログ バックアップに影響します。
- SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.ConfigファイルにあるPredefinedWindowsScriptsDirectoryキーを使用して定義します。

必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

キーの値は、API を介して Swagger から表示できます: API /4.7/configsettings

GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。

ベスト プラクティス: 保持する完全バックアップとログ バックアップの総数に基づいて、セカンダリ保持ポリシーを構成することをお勧めします。セカンダリ保持ポリシーについては、データベースとログが異なるボリュームにある場合はそれぞれのバックアップに3つのSnapshotを保持でき、データベースとログが同じボリュームにある場合はそれぞれのバックアップに2つのSnapshotを保持できることを念頭に置いて設定してください。

- SnapLock
 - [Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで指定した保持日数以下にする必要があります。

Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、ポリシーで指定した数よりも多くのSnapshotが保持される可能性があります。

ONTAP 9.12.1以前のバージョンでは、SnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[ポリシー]をクリックします。
3. *新規*をクリックします。
4. 「名前」 ページで、ポリシー名と詳細を入力します。
5. 「バックアップ タイプとレプリケーション」 ページで、次の手順を実行します。
 - a. バックアップ タイプを選択します。

状況	操作
データベース ファイルと必要なトランザクション ログをバックアップ	*完全バックアップとログバックアップ*を選択します。 データベースはログを切り捨てるかたちでバックアップされ、切り捨てられたログを含むすべてのログがバックアップされます。  これは推奨されるバックアップ タイプです。
データベース ファイルとコミットされていないトランザクション ログをバックアップ	*完全バックアップ*を選択します。 データベースはログを切り捨てるかたちでバックアップされ、切り捨てられたログはバックアップされません。
すべてのトランザクション ログをバックアップ	*ログバックアップ*を選択します。 アクティブ ファイルシステム上のすべてのトランザクション ログがバックアップされ、ログの切り捨ては行われません。 ライブ ログと同じディスクに <i>scebackupinfo</i> ディレクトリが作成されます。このディレクトリには、Exchangeデータベースの変更内容の差分へのポインタが格納されており、完全なログ ファイルとは異なります。
トランザクション ログ ファイルの切り捨てなしで、すべてのデータベース ファイルとトランザクション ログをバックアップ	*バックアップのコピー*を選択します。 すべてのデータベースとすべてのログがバックアップされ、ログの切り捨ては行われません。通常このタイプのバックアップは、レプリカの再シードのほか、問題のテストや診断のために使用します。



ログ バックアップに必要なスペースは、最新の状態（UTM）保持設定ではなく、フルバックアップ保持設定に基づいて定義する必要があります。



Exchangeボリューム（LUN）を扱う場合は、ログとデータベースに個別のバックアップ ポリシーを作成して、同じラベルを使用し、ラベルごとにログ ポリシーのkeep（保持）の値をデータベース ポリシーの値の2倍に設定します。詳細については、["SnapCenter for Exchange バックアップは、Vault の宛先ログボリュームにスナップショットの半分のみを保存します。"](#)

b. [Database Availability Group Settings]セクションで、操作を選択します。

フィールド	操作
アクティブコピーをバックアップする	選択したデータベースのアクティブ コピーのみをバックアップする場合は、このオプションを選択します。 データベース可用性グループ（DAG）については、DAG内のすべてのデータベースのアクティブ コピーのみがバックアップされます。 パッシブ コピーはバックアップされません。
Back up copies on servers to be selected at backup job creation time	選択したサーバ上のデータベースのコピー（アクティブとパッシブの両方）をバックアップする場合は、このオプションを選択します。 DAGについては、選択したサーバ上のすべてのデータベースのアクティブ コピーとパッシブ コピーの両方がバックアップされます。



クラスタ構成では、ポリシーで設定された保持設定に従って、バックアップがクラスタの各ノードに保持されます。クラスタの所有者ノードが変更された場合、以前の所有者ノードのバックアップが保持されます。保持設定はノード レベルでのみ適用されます。

- c. スケジュール頻度セクションで、オンデマンド、時間別、日次、週次、*月次*の 1 つ以上の頻度タイプを選択します。



リソース グループを作成する際に、バックアップ処理のスケジュール（開始日と終了日）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソース グループを作成できますが、各ポリシーに異なるバックアップ スケジュールを割り当てることもできます。



午前 2 時にスケジュールを設定した場合、夏時間 (DST) 中はスケジュールは実行されません。

- a. ポリシーラベルを選択します。



リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしなくても実行できます。

- b. [セカンダリ レプリケーション オプションの選択] セクションで、次のセカンダリ レプリケーション オプションの 1 つまたは両方を選択します。

フィールド	操作
Update SnapMirror after creating a local Snapshot	別のボリュームにバックアップ セットのミラー コピーを保持する場合 (SnapMirror) は、このオプションを選択します。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。 このオプションは、SnapMirrorアクティブ同期に対して有効にする必要があります。  Exchange ONTAPボリュームに対してSnapMirrorアクティブ同期が設定されている場合は、プライマリのみのポリシーは使用できません。SnapCenterではこれが許可されていません。「Mirror」オプションを有効にする必要があります。 トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 見る"TopologyページでのExchangeバックアップの表示"]。
Update SnapVault after creating a local Snapshot	ディスクツーディスクのバックアップ レプリケーションを実行する場合は、このオプションを選択します。
Error retry count	レプリケーションの最大試行回数を入力します。この回数を超えると処理が停止します。



セカンダリ ストレージでSnapshotの上限に達しないように、ONTAPでセカンダリ ストレージのSnapMirror保持ポリシーを設定する必要があります。

6. [Retention]ページで、保持設定を指定します。

表示されるオプションは、前に選択したバックアップ タイプと頻度タイプによって異なります。



最大保持値は 1018 です。保持数を、使用しているONTAPバージョンがサポートする値よりも大きい値に設定すると、バックアップが失敗します。



SnapVaultレプリケーションを有効にする場合は、保持数を2以上に設定する必要があります。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。

- a. [Log backups retention settings]セクションで、次のいずれかを選択します。

状況	操作
特定の数のログ バックアップのみを保持	*ログが保持される完全バックアップの数*を選択し、最新の状態に復元可能な完全バックアップの数を指定します。 最新の状態（UTM）保持設定は、フル バックアップまたはログ バックアップを通じて作成されたログ バックアップに適用されます。たとえば、UTM保持設定が過去5回分のフル バックアップのログ バックアップを保持するようになっている場合、過去5回分のフル バックアップのログ バックアップが保持されます。 フル / ログ バックアップの一部として作成されたログ フォルダは、UTM処理の流れの中で自動的に削除されます。ログ フォルダを手動で削除することはできません。たとえば、フル バックアップやフル / ログ バックアップの保持設定が1か月に設定され、UTM保持期間が10日に設定されている場合、これらのバックアップの一環として作成されたログ フォルダは、UTM保持設定に従って削除されます。そのため、ログ フォルダは10日間しか保持されず、その他のバックアップはすべてポイントインタイム リストアの対象としてマークされます。 最新の状態へのリストアを実行しない場合は、UTM保持設定の値を0に設定します。これにより、ポイントインタイム リストア処理が有効になります。 ベスト プラクティス: この設定は、完全バックアップの保持設定セクションのスナップショットの合計数 (完全バックアップ) の設定と同じにすることが最適です。これにより、フル バックアップごとにログ ファイルが保持されます。
バックアップ コピーを特定の日数だけ保持	最後のログ バックアップを保持する オプションを選択し、ログ バックアップ コピーを保持する日数を指定します。 フル バックアップが保持される日数まで、ログ バックアップが保持されます。
Snapshot locking period	*スナップショット コピーのロック期間*を選択し、日、月、または年を選択します。 SnapLock保持期間は100年未満にする必要があります。

バックアップ タイプとして [ログ バックアップ] を選択した場合、ログ バックアップは完全バックアップの最新保持設定の一部として保持されます。

- b. [Full backup retention settings]セクションで、次のいずれかをオンデマンド バックアップ用を選択し、続けてフル バックアップ用にもいずれかを選択します。

フィールド	操作
Retain only a specific number of Snapshots	保持する完全バックアップの数を指定する場合は、「保持するスナップショット コピーの合計数」オプションを選択し、保持するスナップショット (完全バックアップ) の数を指定します。 フル バックアップの数が指定した数を超えると、指定した数を超えるフル バックアップが、最も古いコピーから順に削除されます。
Retain full backups for a specific number of days	スナップショット コピーの保存期間 オプションを選択し、スナップショット (完全バックアップ) を保存する日数を指定します。
プライマリスナップショットのロック期間	*プライマリ スナップショット コピーのロック期間*を選択し、日、月、または年を選択します。 SnapLock保持期間は100年未満にする必要があります。
セカンダリスナップショットのロック期間	*セカンダリ スナップショット コピーのロック期間*を選択し、日、月、または年を選択します。

DAG構成のホストにフル バックアップがなくログ バックアップのみのデータベースがある場合は、次の方法でログ バックアップが保持されます。

- デフォルトでは、SnapCenter はDAG 内の他のすべてのホストでこのデータベースの最も古い完全バックアップを見つけ、完全バックアップの前にこのホストで作成されたすべてのログ バックアップを削除します。
- C:\Program Files\NetApp\ SnapCenter WebApp\web.config ファイルにキー **MaxLogBackupOnlyCountWithoutFullBackup** を追加することで、ログ バックアップのみを使用する DAG 内のホスト上のデータベースに対する上記のデフォルトの保持動作をオーバーライドできます。

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

この例では、値が10になっています。これは、ホストで保持できるログ バックアップが最大10個であることを意味します。

7. [Script]ページで、バックアップ処理の前またはあとに実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

- プレスクリプトのバックアップ引数には、「\$Database」と「\$ServerInstance」が含まれます。
- PostScript バックアップ引数には、「\$Database」、「\$ServerInstance」、「\$BackupName」、「\$LogDirectory」、および「\$LogSnapshot」が含まれます。

SNMPトラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。



プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

8. 概要を確認し、[完了] をクリックします。

Exchange Serverのリソース グループの作成とポリシーの適用

リソース グループはいずれのデータ保護ジョブにも必要になります。リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプと保護スケジュールを定義することも必要です。

タスク概要

- SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.ConfigファイルにあるPredefinedWindowsScriptsDirectoryキーを使用して定義します。

必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

キーの値は、API を介して Swagger から表示できます: API /4.7/configsettings

GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期を使用するリソースを含む既存のリソース グループにSnapMirrorアクティブ同期を使用しない新しいデータベースを追加することはできません。
- SnapMirrorアクティブ同期のフェイルオーバー モードである既存のリソース グループに新しいデータベースを追加することはできません。リソースを追加できるのは、通常の状態またはフェイルバック状態のリソース グループのみです。

手順

1. 左側のナビゲーション ウィンドウで [リソース] をクリックし、リストから Microsoft Exchange Server プラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] を選択します。



SnapCenterに最近リソースを追加した場合は、[リソースの更新] をクリックして、新しく追加されたリソースを表示します。

3. *新しいリソース グループ*をクリックします。
4. [Name]ページで、次の操作を実行します。

フィールド	操作
Name	リソース グループ名を入力します。  リソース グループ名は250文字以内で指定する必要があります。
Tags	リソース グループを検索しやすくするために、ラベルを入力します。 たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。
Use custom name format for Snapshot copy	オプション: カスタム スナップショットの名前と形式を入力します。 たとえば、<i>customtext_resourcegroup_policy_hostname</i> または <i>resourcegroup_hostname</i> です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

5. [Resources]ページで、次の手順を実行します。

- a. リソース タイプとデータベース可用性グループをドロップダウン リストから選択し、使用可能なリソースのリストをフィルタします。



最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources]のリストには表示されません。

[Available Resources]セクションと[Selected Resources]セクションに、データベース名がホストの完全修飾ドメイン名 (FQDN) とともに表示されます。このFQDNは、データベースが特定のホスト上でアクティブであり、このホスト上にはバックアップが作成されない可能性があることを示すためのものです。ポリシーで「バックアップ ジョブの作成時に選択されるサーバー上のコピーをバックアップする」オプションを選択した場合は、バックアップを実行するサーバー選択オプションから 1 つ以上のバックアップ サーバーを選択する必要があります。

- b. 検索テキスト ボックスにリソースの名前を入力するか、スクロールしてリソースを見つけます。
- c. 次のいずれかの手順を実行し、リソースを[Available Resources]セクションから[Selected Resources]セクションに移動します。
 - 同じボリューム上のすべてのリソースを「選択したリソース」セクションに移動するには、「同じストレージ ボリューム上のすべてのリソースを自動選択」を選択します。
 - 「利用可能なリソース」セクションからリソースを選択し、右矢印をクリックして「選択したリソース」セクションに移動します。

SnapCenter for Microsoft Exchange Serverのリソース グループに含めることができるデータベースの数は、1つのSnapshotにつき最大30個です。1つのリソース グループに30個を超えるデータベースがある場合は、超過分のデータベース用に2つ目のSnapshotが作成されます。それに伴い、メ

インのバックアップ ジョブの下に2つのサブジョブが作成されます。セカンダリ レプリケーションが設定されたバックアップで、SnapMirrorやSnapVaultの更新中に、両方のサブジョブの更新が同時に実行される場合があります。ログにジョブの完了が記録されている場合でも、メインのバックアップ ジョブは無期限に実行され続けます。

6. [Policies]ページで、次の手順を実行します。

a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます 。



ポリシーに「バックアップ ジョブの作成時に選択されるサーバー上のコピーをバックアップする」オプションが含まれている場合は、1 つ以上のサーバーを選択するためのサーバー選択オプションが表示されます。サーバ選択オプションには、選択したデータベースがNetAppストレージ上にあるサーバのみが表示されます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. 選択したポリシーのスケジュールを構成するセクションで、 * スケジュールを構成するポリシーの *[スケジュールの構成] 列で、
- c. [ポリシー *policy_name* のスケジュールの追加] ダイアログ ボックスで、開始日、有効期限、頻度を指定してスケジュールを構成し、[OK] をクリックします。

この操作は、ポリシーに指定されている頻度ごとに実行する必要があります。構成されたスケジュールは、[選択したポリシーのスケジュールを構成する] セクションの [適用されたスケジュール] 列に表示されます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

7. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。

電子メール通知の場合は、GUIまたはPowerShellコマンドを使用してSMTPサーバーの詳細を指定する必要があります。 `Set-SmSmtServer`。

コマンドレットで使用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

8. 概要を確認し、[完了] をクリックします。

Exchange Server用のPowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成

PowerShellコマンドレットを使用してバックアップとリストアを実行する前に、Storage Virtual Machine (SVM) 接続とクレデンシャルを作成する必要があります。

開始する前に

- PowerShellコマンドレットを実行できるようにPowerShell環境を準備しておく必要があります。
- ストレージ接続を作成するには、Infrastructure Adminロールの権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

ストレージ システム接続の追加中は、ホスト プラグインのインストールが進行中であってはなりません。ホスト キャッシュが更新されず、 SnapCenter GUI にデータベースのステータスが「バックアップに使用できません」または「NetAppストレージ上にありません」と表示される可能性があるためです。

- ストレージ システムの名前は一意である必要があります。

SnapCenterでは、別々のクラスタに属している場合でも、複数のストレージ システムに同じ名前を付けることはサポートされません。SnapCenterでサポートする各ストレージ システムには、一意な名前とデータLIFの一意なIPアドレスが必要です。

手順

1. PowerShell接続セッションを開始するには、`Open-SmConnection`コマンドレット。

PowerShellセッションを開く例を次に示します。

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

2. ストレージシステムへの新しい接続を作成するには、`Add-SmStorageConnection`コマンドレット。

新しいストレージ システム接続を作成する例を次に示します。

```
PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https  
-Timeout 60
```

3. 新しい実行アカウントを作成するには、`Add-Credential`コマンドレット。

Windowsクレデンシャルを使用してExchangeAdminという名前の新しいRun Asアカウントを作成する例を次に示します。

```
PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows  
-Credential sddev\administrator
```

コマンドレットで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

Exchangeデータベースのバックアップ

データベースがどのリソース グループにも含まれていない場合は、[Resources]ページからデータベースまたはデータベース可用性グループをバックアップできます。

開始する前に

- バックアップ ポリシーを作成しておく必要があります。
- バックアップ処理で使用するアグリゲートを、データベースが使用するSVMに割り当てておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合、ストレージ ユーザーに割り当てられているロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。
- NetAppおよび非NetAppストレージ上にアクティブ/パッシブ データベース コピーを持つデータベースまたはデータベース可用性グループのバックアップを実行する場合、ポリシーで アクティブ コピーをバックアップする または バックアップ ジョブの作成時に選択されるサーバー上のコピーをバックアップする オプションを選択すると、バックアップ ジョブは警告状態になります。NetAppストレージ上のアクティブ/パッシブ データベース コピーのバックアップは成功し、他社ストレージ上のアクティブ/パッシブ データベース コピーのバックアップは失敗します。

ベスト プラクティス: アクティブ データベースとパッシブ データベースのバックアップを同時に実行しないでください。競合状態が発生し、いずれかのバックアップが失敗する可能性があります。

SnapCenter UI

手順

1. 左側のナビゲーション ウィンドウで、[リソース] をクリックし、リストから **[Microsoft Exchange Server プラグイン]** を選択します。
2. [リソース] ページで、[表示] リストから [データベース] または [データベース可用性グループ] を選択します。

リソースページでは、 アイコンは、データベースがNetApp以外のストレージ上にあることを示します。



DAG内で、アクティブ データベース コピーが他社ストレージにあり、1つ以上のパッシブ データベース コピーがNetAppストレージにある場合は、データベースを保護できます。

クリック  *、ホスト名とデータベース タイプを選択してリソースをフィルターします。*をクリックします  フィルター パネルを閉じます。

- データベースをバックアップする場合は、データベース名をクリックします。
 - i. トポロジ ビューが表示されている場合は、[保護] をクリックします。
 - ii. [Database - Protect Resource]ウィザードが表示された場合は、手順3に進みます。
 - データベース可用性グループをバックアップする場合は、データベース可用性グループの名前をクリックします。
3. カスタム スナップショット名を指定する場合は、[リソース] ページで [スナップショット コピーにカスタム名形式を使用する] チェック ボックスをオンにし、スナップショット名に使用するカスタム名形式を入力します。

たとえば、*customtext_policy_hostname* または *resource_hostname* です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

4. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます  。



ポリシーに「バックアップ ジョブの作成時に選択されるサーバー上のコピーをバックアップする」オプションが含まれている場合、1つ以上のサーバーを選択するためのサーバー選択オプションが表示されます。サーバ選択オプションでは、選択したデータベースがNetAppストレージ上にあるサーバのみが表示されます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. クリック *  * スケジュールを構成するポリシーの [スケジュールの構成] 列で、
- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリ

ックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

5. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースに対して実行されたバックアップ操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

6. 概要を確認し、[完了] をクリックします。

データベース トポロジのページが表示されます。

7. *今すぐバックアップ*をクリックします。

8. [Backup]ページで次の手順を実行します。

- a. リソースに複数のポリシーを適用している場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*をクリックします。

9. バックアップの進捗状況を監視するには、ページ下部の[Activity]ペインでジョブをダブルクリックして[Job Details]ページを表示します。

- MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

詳細については、以下を参照してください。 ["MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"](#)

- VMDK上のアプリケーション データをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープ サイズが不足していると、バックアップが失敗することがあります。

Java ヒープ サイズを増やすには、スクリプト ファイル `/opt/netapp/init_scripts/scvservice` を見つけます。このスクリプトでは、`do_start method` コマンドによってSnapCenter VMware プラグイン サービスが開始されます。このコマンドを次のように更新します: `Java -jar -Xmx8192M -Xms4096M`

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-smconnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmPolicyコマンドレットを使用して、バックアップ ポリシーを作成します。

この例では、Exchangeのバックアップ タイプとしてフル バックアップとログ バックアップを指定して新しいバックアップ ポリシーを作成しています。

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy  
-PolicyType Backup -PluginPolicytype SCE -SceBackupType  
FullBackupAndLogBackup -BackupActiveCopies
```

この例では、Exchangeのバックアップ タイプとして1時間ごとのフル バックアップとログ バックアップを指定して新しいバックアップ ポリシーを作成しています。

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy  
-PolicyType Backup -PluginPolicytype SCE -SceBackupType  
FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly  
-RetentionSettings  
{ 'BackupType'='DATA'; 'ScheduleType'='Hourly'; 'RetentionCount'='10' }
```

この例では、Exchangeログのみをバックアップする新しいバックアップ ポリシーを作成しています。

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup  
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

3. Get-SmResourcesコマンドレットを使用してホスト リソースを検出します。

この例では、指定したホスト上でMicrosoft Exchange Serverプラグインのリソースを検出しています。

```
C:\PS> Get-SmResources -HostName vise-f6.sddev.mycompany.com  
-PluginCode SCE
```

4. Add-SmResourceGroupコマンドレットを使用して、SnapCenterに新しいリソース グループを追加します。

この例では、ポリシーとリソースを指定して新しいExchange Serverデータベース バックアップ リソース グループを作成しています。

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

この例では、ポリシーとリソースを指定して新しいExchangeデータベース可用性グループ (DAG) のバックアップ リソース グループを作成しています。

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode
SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database Availability Group";"Names"="DAGSCE0102"}
```

5. New-SmBackupコマンドレットを使用して、新しいバックアップ ジョブを開始します。

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

この例では、セカンダリ ストレージに新しいバックアップを作成しています。

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

6. Get-SmBackupReportコマンドレットを使用して、バックアップ ジョブのステータスを表示します。

この例では、指定した日に実行されたすべてのジョブの概要レポートを表示しています。

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

この例では、ジョブIDを指定してジョブ サマリ レポートを表示しています。

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。または、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

Exchangeリソース グループのバックアップ

リソース グループは、ホストまたはExchange DAG上のリソースの集まりであり、リソース グループにはDAG全体または個々のデータベースを含めることができます。リソース グループは、[Resources]ページでバックアップできます。

開始する前に

- ポリシーを適用したリソース グループを作成しておく必要があります。
- バックアップ処理で使用されるアグリゲートを、データベースが使用するStorage Virtual Machine (SVM) に割り当てておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合、ストレージ ユーザーに割り当てられているロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。
- リソース グループにホストが異なる複数のデータベースが含まれている場合、ネットワークの問題が原因で、一部のホストでのバックアップ処理の開始が遅れることがあります。の値を設定する必要があります。`MaxRetryForUninitializedHosts`で`web.config`を使用することにより`Set-SmConfigSettings` PowerShell コマンドレット。
- リソース グループに、NetAppおよび非NetAppストレージ上にアクティブ/パッシブ データベース コピーを持つデータベースまたはデータベース可用性グループを含め、ポリシーで アクティブ コピーをバックアップ または バックアップ ジョブの作成時に選択されるサーバー上のコピーをバックアップ オプションを選択した場合、バックアップ ジョブは警告状態になります。

NetAppストレージ上のアクティブ / パッシブ データベース コピーのバックアップは成功し、他社ストレージ上のアクティブ / パッシブ データベース コピーのバックアップは失敗します。

タスク概要

リソース グループは、[Resources]ページからオンデマンドでバックアップできます。リソース グループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが行われます。

手順

1. 左側のナビゲーション ウィンドウで、[リソース] をクリックし、リストから **[Microsoft Exchange Server プラグイン]** を選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。

リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、をクリックします。 *、タグを選択します。*をクリックします フィルター パネルを閉じます。

3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] をクリックします。
4. [Backup]ページで次の手順を実行します。
 - a. リソース グループに複数のポリシーを関連付けている場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*をクリックします。
5. バックアップの進捗状況を監視するには、ページ下部の[Activity]ペインでジョブをダブルクリックして[Job Details]ページを表示します。

バックアップ処理の監視

SnapCenterの[Jobs]ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*ジョブ*をクリックします。
3. [Jobs]ページで、次の手順を実行します。
 - a. をクリックして、 リストの内容をバックアップ処理だけに絞り込みます。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*バックアップ*を選択します。
 - d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. バックアップ ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスは  ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[Activity]ペインでの処理の監視

[Activity]ペインには、最後に実行された5つの処理が表示されます。また[Activity]ペインには、処理が開始された日次と処理のステータスが表示されます。

[Activity]ペインには、バックアップ、リストア、クローニング、スケジュールされたバックアップの各処理に関する情報が表示されます。

手順

- 1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
- 2. クリック  アクティビティ ペインで、最新の 5 つの操作を表示します。

いずれかの操作をクリックすると、*ジョブの詳細*ページに操作の詳細が表示されます。

Exchangeデータベースのバックアップ処理のキャンセル

キューに登録されているバックアップ処理はキャンセルできます。

必要なもの

- 処理をキャンセルするには、SnapCenter管理者かジョブ所有者としてログインする必要があります。
- バックアップ操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のバックアップ処理はキャンセルできません。
- バックアップ処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。
- キャンセルできない操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたバックアップ操作をキャンセルできます。

手順

- 1. 次のいずれかを実行します。

方法	アクション
[Monitor]ページ	a. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 b. 操作を選択し、「ジョブのキャンセル」をクリックします。

方法	アクション
[Activity]ペイン	- バックアップ操作を開始したら、*をクリックします。 * アクティビティ ペインで、最新の5つの操作を表示します。 - 処理を選択します。 - ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

処理がキャンセルされ、リソースは処理前の状態に戻ります。

[Topology]ページでのExchangeバックアップの表示

リソースのバックアップを準備する際に、プライマリ ストレージとセカンダリ ストレージ上のすべてのバックアップの図を表示すると役に立ちます。

タスク概要

[Topology]ページに、選択したリソースまたはリソース グループに使用できるバックアップをすべて表示できます。これらのバックアップの詳細を参照し、対象を選択してデータ保護処理を実行できます。

プライマリ ストレージまたはセカンダリ ストレージ（ミラー コピーまたはバックアップ コピー）にバックアップがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

- 
 プライマリ ストレージで使用可能なバックアップの数を表示します。
- 
 SnapMirrorテクノロジーを使用してセカンダリ ストレージにミラーリングされているバックアップの数を表示します。
- 
 SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップの数を表示します。

- 表示されるバックアップの数には、セカンダリ ストレージから削除されたバックアップも含まれます。

たとえば、バックアップを4個保持するポリシーを使用してバックアップを6個作成した場合、バックアップの数は6個と表示されます。

ベスト プラクティス: 複製されたバックアップの正しい数が表示されるようにするには、トポロジを更新することをお勧めします。

SnapMirrorアクティブ同期 (当初はSnapMirror Business Continuity [SM-BC] としてリリース) としてセカンダリ関係がある場合は、次の追加アイコンが表示されます。

- 



レプリカサイトが稼働しています。



レプリカサイトはダウンしています。



セカンダリ ミラーまたはボールド関係が再確立されていません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストからデータベース、リソース、またはリソース グループを選択します。
3. データベースの詳細ビューまたはリソース グループの詳細ビューで、リソースを選択します。

リソースが保護されている場合は、選択したリソースの[Topology]ページが表示されます。

4. [Summary Card]セクションで、プライマリ ストレージとセカンダリ ストレージ上にあるバックアップ数の概要を確認します。

[Summary Card]セクションには、バックアップの総数およびログ バックアップの総数が表示されます。

更新 ボタンをクリックすると、ストレージのクエリが開始され、正確な数が表示されます。

SnapLock対応バックアップが取得された場合、[更新] ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでも、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

アプリケーション リソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限はONTAPから取得されます。

SnapMirrorアクティブ同期の場合、[更新] ボタンをクリックすると、プライマリ サイトとレプリカ サイトの両方に対してONTAPを照会してSnapCenterバックアップ インベントリが更新されます。週次スケジュールでも、SnapMirrorアクティブ同期関係を含むすべてのデータベースに対してこの処理が実行されます。

- SnapMirrorアクティブ同期とONTAP（バージョン9.14.1のみ）では、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップの関係については、フェイルオーバー後に手動で設定する必要があります。ONTAP 9.15.1以降は、新しいプライマリ デスティネーションに対するフェイルオーバー後の非同期ミラーまたは非同期ミラー バックアップが、自動的に設定されます。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。バックアップが作成された後にのみ、「更新」をクリックできます。

5. 「コピーの管理」ビューで、プライマリ ストレージまたはセカンダリ ストレージから バックアップ をクリックして、バックアップの詳細を表示します。

バックアップの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、名前変更、削除の各処理を実行します。



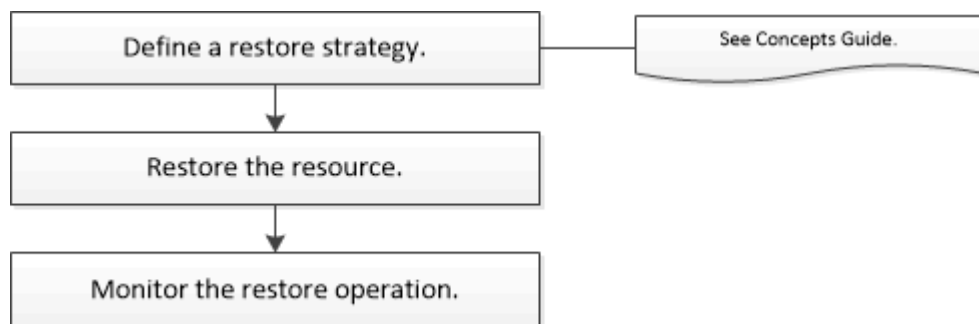
セカンダリ ストレージ上のバックアップは、名前変更または削除できません。Snapshotの削除は、ONTAPの保持設定で処理されます。

Exchangeリソースのリストア

リストアのワークフロー

SnapCenterを使用して、1つ以上のバックアップをアクティブ ファイルシステムにリストアすることにより、Exchangeデータベースをリストアすることができます。

次のワークフローは、Exchangeデータベースのリストア処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトでを使用して、バックアップとリストアの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterコマンドレットのヘルプを使用するか、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

Exchangeデータベースをリストアする際の要件

SnapCenter Plug-in for Microsoft Exchange ServerのバックアップからExchange Serverデータベースをリストアする前に、以下の要件を満たしていることを確認する必要があります。



すべてのリストア機能を使用するには、SnapCenter ServerとSnapCenter Plug-in for Exchangeデータベースの両方を4.6にアップグレードする必要があります。

- Exchange Serverがオンラインで、稼働している必要があります。
- データベースがExchange Server上に存在している必要があります。



削除したデータベースのリストアはサポートされていません。

- データベースのSnapCenterスケジュールは、一時停止する必要があります。
- SnapCenter ServerとSnapCenter Plug-in for Microsoft Exchange Serverホストが、リストア対象のバックアップが格納されているプライマリ ストレージとセカンダリ ストレージに接続されている必要があります。

Exchangeデータベースのリストア

SnapCenterを使用して、バックアップされたExchangeデータベースをリストアすることができます。

開始する前に

- リソース グループ、データベース、またはデータベース可用性グループ (DAG) をバックアップしておく必要があります。
- Exchangeデータベースを別の場所に移行した場合、古いバックアップに対するリストア処理は実行できません。
- Snapshotをミラーまたはバックアップにレプリケートするユーザには、SnapCenter管理者がユーザに対してソースとデスティネーションの両方のボリューム用にSVMを割り当てる必要があります。
- DAG内で、アクティブ データベース コピーが他社ストレージにある場合に、NetAppストレージにあるパッシブ データベース コピーのバックアップからリストアするには、そのパッシブ コピー (NetAppストレージ) をアクティブ コピーとして設定し、リソースを更新してリストア処理を実行します。

実行 `Move-ActiveMailboxDatabase` パッシブ データベース コピーをアクティブ データベース コピーとして作成するコマンド。

その "[Microsoftのドキュメント](#)"このコマンドに関する情報が含まれています。

タスク概要

- データベースに対してリストア処理を実行すると、データベースは同じホストに再マウントされ、新しいボリュームは作成されません。
- DAGレベルのバックアップは、個々のデータベースからリストアする必要があります。
- Exchangeデータベース (.edb) ファイル以外のファイルが存在する場合、フル ディスク リストアはサポートされません。

レプリケーションに使用するファイルなどのExchangeファイルが含まれているディスクでは、Plug-in for Exchangeによるディスクのフル リストアは実行されません。フル リストアがExchangeの機能に影響を及ぼす可能性がある場合、Plug-in for Exchangeにより単一ファイルのリストア処理が実行されます。

- Plug-in for Exchangeでは、BitLockerで暗号化されたドライブはリストアできません。
- SCRIPTS_PATHは、プラグイン ホストのSMCoreServiceHost.exe.ConfigファイルにあるPredefinedWindowsScriptsDirectoryキーを使用して定義します。

必要に応じて、このパスを変更してSMcoreサービスを再起動できます。セキュリティを確保するために、デフォルトのパスを使用することを推奨します。

キーの値は、API を介して Swagger から表示できます: [API /4.7/configsettings](#)

GET APIを使用すると、キーの値を表示できます。SET APIはサポートされません。

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期でリストア処理を実行するには、プライマリの場所からバックアップを選択する必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで、リソース ページの左上隅にある リソース をクリックします。
2. ドロップダウン リストからExchange Serverプラグインを選択します。
3. [リソース] ページで、[表示] リストから データベース を選択します。
4. リストからデータベースを選択します。
5. コピーの管理ビューで、プライマリバックアップテーブルから*バックアップ*を選択し、*をクリックします。*。
6. [Options]ページで、次のいずれかのログ バックアップ オプションを選択します。

オプション	説明
All log backups	完全バックアップ後に利用可能なすべてのログ バックアップを復元するために、最新のバックアップ復元操作を実行するには、[すべてのログ バックアップ]を選択します。
By log backups until	ポイントインタイム復元操作を実行するには、[ログ バックアップまで]を選択します。これにより、選択したログまでのログ バックアップに基づいてデータベースが復元されます。  ドロップダウン リストに表示されるログの数は、UTMに基づきます。たとえば、フル バックアップの保持数が5でUTMの保持数が3の場合、使用可能なログ バックアップの数は5ですが、ドロップダウンにはリストア処理を実行できるログが3つだけ表示されます。
By specific date until	復元されたデータベースにトランザクション ログが適用される日時を指定するには、[特定の日付まで]を選択します。このポイントインタイム リストア処理では、指定した日時のバックアップまでに記録されたトランザクション ログのエントリがリストアされます。
None	ログ バックアップなしで完全バックアップのみを復元する必要がある場合は、[なし]を選択します。

次のいずれかを実行します。

- 復元後にデータベースを回復してマウントする - このオプションはデフォルトで選択されています。

- 。復元前にバックアップ内のトランザクション ログの整合性を検証しない - デフォルトでは、SnapCenter は復元操作を実行する前に、バックアップ内のトランザクション ログの整合性を検証します。

ベストプラクティス: このオプションは選択しないでください。

7. [Script]ページで、リストア処理の前またはあとに実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。

リストア プリスクリプトの引数には、\$Databaseと\$ServerInstanceがあります。

リストア ポストスクリプトの引数には、\$Database、\$ServerInstance、\$BackupName、\$LogDirectory、\$TargetServerInstanceがあります。

SNMPトラップの更新、アラートの自動化、ログの送信などをスクリプトで実行できます。



プリスクリプトやポストスクリプトのパスに、ドライブや共有を含めることはできません。パスは、SCRIPTS_PATHの相対パスである必要があります。

8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。

9. 概要を確認し、[完了] をクリックします。

10. ページ下部の[Activity]パネルを展開すると、リストア ジョブのステータスを表示できます。

モニター > ジョブ ページを使用して、復元プロセスを監視する必要があります。

レプリカとアクティブ データベースの間に遅延がある場合に、バックアップからアクティブ データベースをリストアすると、パッシブ データベースが一時停止状態または障害状態になることがあります。

状態の変化は、アクティブ データベースのログ チェーンがフォークし、レプリケーションを中断する新しいブランチが開始されたときに発生します。Exchange Serverによりレプリカの修正が試みられますが、修正できない場合は、リストア後に新しいバックアップを作成し、レプリカを再シードする必要があります。

PowerShellコマンドレット

手順

1. 指定されたユーザーに対してSnapCenter Serverとの接続セッションを開始するには、`Open-SmConnection`コマンドレット。

```
Open-smconnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

2. 復元したい1つ以上のバックアップに関する情報を取得するには、`Get-SmBackup`コマンドレット。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。


```
PS C:\> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
-----	-----
341	ResourceGroup_36304978_UTM...
12/8/2017 4:13:24 PM	Full Backup
342	ResourceGroup_36304978_UTM...
12/8/2017 4:16:23 PM	Full Backup
355	ResourceGroup_06140588_UTM...
12/8/2017 6:32:36 PM	Log Backup
356	ResourceGroup_06140588_UTM...
12/8/2017 6:36:20 PM	Full Backup

3. バックアップからデータを復元するには、`Restore-SmBackup`コマンドレット。

この例では、最新の状態へのバックアップをリストアしています。

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341  
-IsRecoverMount:$true
```

この例では、ポイントインタイム バックアップをリストアしています。

```
C:\ PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341  
-IsRecoverMount:$true -LogRestoreType ByTransactionLogs -LogCount 2
```

この例では、セカンダリ ストレージのバックアップをプライマリ ストレージにリストアしています。

```
C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2'  
-BackupId 81 -IsRecoverMount:$true -Confirm:$false  
-archive @{Primary="paw_vs:vol1";Secondary="paw_vs:vol1_mirror"}  
-logrestoretype All
```

その`-archive`パラメータを使用すると、復元に使用するプライマリ ボリュームとセカンダリ ボリュームを指定できます。

その`-IsRecoverMount:\$true`パラメータを使用すると、復元後にデータベースをマウントできます。

コマンドレットで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

メールとメールボックスのきめ細かなリカバリ

Single Mailbox Recovery (SMBR) ソフトウェアを使用すると、Exchangeデータベース全体ではなく、メールやメールボックスの単位でリストアとリカバリを実行できます。

1件のメールをリカバリするためだけにデータベース全体をリストアするのは、大量の時間とリソースを消費することになります。SMBRを使用すると、Snapshotのクローン コピーを作成し、Microsoft APIを使用してSMBRにメールボックスをマウントすることで、メールを迅速にリカバリできます。SMBRの使い方については、"[SMBR 管理ガイド](#)"。

SMBRの追加情報については、次の資料を参照してください。

- "[SMBRで単一アイテムを手動でリストアする方法 \(Ontrack PowerControlsのリストアにも適用可能\)](#)"
- "[SnapCenterを使用してSMBRのセカンダリストレージから復元する方法](#)"
- "[SMBR を使用してSnapVaultから Microsoft Exchange メールを回復する](#)"

セカンダリ ストレージからのExchange Serverデータベースのリストア

バックアップしたExchange Serverデータベースは、セカンダリ ストレージ（ミラーまたはバックアップ） からリストアできます。

プライマリ ストレージからセカンダリ ストレージにSnapshotをレプリケートしておく必要があります。

タスク概要

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期でリストア処理を実行するには、プライマリの場所からバックアップを選択する必要があります。

手順

1. 左側のナビゲーション ウィンドウで、[リソース] をクリックし、リストから **[Microsoft Exchange Server プラグイン]** を選択します。
2. [リソース] ページで、[表示] ドロップダウン リストから [データベース] または [リソース グループ] を選択します。
3. データベースまたはリソース グループを選択します。

データベースまたはリソース グループのトポロジ ページが表示されます。

4. [コピーの管理] セクションで、セカンダリ ストレージ システム (ミラーまたはボルト) から [バックアップ] を選択します。
5. リストからバックアップを選択し、クリックします 。

6. [Location]ページで、選択したリソースをリストアするデスティネーション ボリュームを選択します。
7. 復元ウィザードを完了し、概要を確認して、[完了] をクリックします。

Exchangeのパッシブ ノード レプリカの再シード

コピーの破損時など、レプリカ コピーを再シードする必要がある場合は、SnapCenterの再シード機能を使用して最新のバックアップに再シードできます。

開始する前に

再シードするデータベースのバックアップを作成しておく必要があります。

+ ノード間の遅延を回避するには、再シード操作を実行する前に新しいバックアップを作成するか、最新のバックアップを持つホストを選択します。

手順

1. 左側のナビゲーション ウィンドウで、[リソース] をクリックし、リストから **[Microsoft Exchange Server プラグイン]** を選択します。
2. [Resources]ページで、[View]リストから適切なオプションを選択します。

オプション	説明
単一のデータベースを再シードする	表示リストから*データベース*を選択します。
DAG内のデータベースを再シードする	表示リストから*データベース可用性グループ*を選択します。

3. 再シードするリソースを選択します。
4. 「コピーの管理」ページで、「再シード」をクリックします。
5. 再シード ウィザードの正常でないデータベース コピーのリストから、再シードするものを選択し、[次へ] をクリックします。
6. ホスト ウィンドウで、再シードするバックアップがあるホストを選択し、[次へ] をクリックします。
7. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。

8. 概要を確認し、[完了] をクリックします。
9. ページ下部の[Activity]パネルを展開すると、ジョブのステータスを表示できます。



パッシブ データベース コピーが他社ストレージにある場合、再シード処理はサポートされません。

Exchangeデータベース用のPowerShellコマンドレットを使用したレプリカの再シード

PowerShellコマンドレットを使用すると、同じホスト上にある最新のコピーまたは代替

ホスト上にある最新のコピーを使用して、正常でないレプリカをリストアできます。

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. 指定されたユーザーに対してSnapCenter Serverとの接続セッションを開始するには、`Open-SmConnection` コマンドレット。

```
Open-smconnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. データベースを再シードするには、`reseed-SmDagReplicaCopy` コマンドレット。

この例では、「mva-rx200.netapp.com」というホストにある、execdbというデータベースの失敗したコピーを、そのホストにある最新のバックアップを使用して再シードしています。

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database  
execdb
```

この例では、「mva-rx201.netapp.com」という代替ホストにある、execdbという名前のデータベースの失敗したコピーを、データベース（本番 / コピー）の最新のバックアップを使用して再シードしています。

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database  
execdb -BackupHost "mva-rx201.netapp.com"
```

リストア処理の監視

[Job]ページを使用して、SnapCenterの各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした

-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター* ページで、*ジョブ* をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  でリストをフィルタリングし、リストア処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ* ドロップダウンリストから*復元*を選択します。
 - d. *ステータス* ドロップダウンリストから、復元ステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. 復元ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細* ページで、*ログの表示* をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

Exchange データベースのリストア処理のキャンセル

キューに登録されているリストア ジョブはキャンセルできます。

リストア処理をキャンセルするには、SnapCenter 管理者かジョブ所有者としてログインする必要があります。

タスク概要

- キューに入れられた復元操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のリストア処理はキャンセルできません。
- キューに登録されているリストア処理のキャンセルには、SnapCenter GUI、PowerShell コマンドレット、または CLI コマンドを使用できます。
- キャンセルできない復元操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられた復元操作をキャンセルできます。

手順

次のいずれかを実行します。

方法	アクション
[Monitor]ページ	1. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 2. ジョブを選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	1. 復元操作を開始したら、 アクティビティ ペインで、最新の 5 つの操作を表示します。 2. 処理を選択します。 3. ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

IBM Db2の保護

SnapCenter Plug-in for IBM Db2

SnapCenter Plug-in for IBM Db2の概要

SnapCenter Plug-in for IBM Db2 Databaseは、IBM Db2データベースに対応したデータ保護管理を提供する、NetApp SnapCenterソフトウェアのホスト側コンポーネントです。Plug-in for IBM Db2 Databaseは、SnapCenter環境でのIBM Db2データベースのバックアップ、リストア、およびクローニングを自動化します。

- SnapCenter 6.0 は IBM Db2 10.5 以降をサポートしています。
- SnapCenter 6.0.1 は IBM Db2 9.7.x 以降をサポートしています。また、SnapCenter 6.0.1 以降では、AIX 上の IBM Db2 がサポートされます。

SnapCenterは、シングル インスタンスおよびマルチ インスタンスのDb2セットアップをサポートしています。Plug-in for IBM Db2 Databaseは、LinuxとWindowsのどちらの環境でも使用できます。Windows環境では、Db2は手動リソースとしてサポートされます。



Db2 pureScale 環境および Db2 マルチノード (DPF) システムはサポートされていません。

Plug-in for IBM Db2 Databaseがインストールされている場合は、SnapCenterとNetApp SnapMirrorテクノロジーを使用して、バックアップ セットのミラー コピーを別のボリュームに作成できます。また、このプラグインをNetApp SnapVaultテクノロジーとともに使用して、標準への準拠を目的としたディスクツーディスク バックアップ レプリケーションを実行することもできます。

SnapCenter Plug-in for Db2は、ONTAPおよびAzure NetApp Filesストレージ レイアウトでNFSとSANをサポートします。

VMDK、vVol、RDM 仮想ストレージ レイアウトがサポートされています。

SnapCenter Plug-in for IBM Db2の機能

Plug-in for IBM Db2 Databaseをインストールした環境では、SnapCenterを使用してIBM Db2データベースとそのリソースをバックアップ、リストア、クローニングできます。これらの処理をサポートするタスクも実行できます。

- データベースを追加します。
- バックアップを作成します。
- バックアップからリストアします。
- バックアップをクローニングします。
- バックアップ処理のスケジュールを設定します。
- バックアップ、リストア、クローニングの各処理を監視します。
- バックアップ、リストア、クローニングの各処理のレポートを表示します。

SnapCenter Plug-in for IBM Db2の特長

SnapCenterは、プラグイン アプリケーションと統合されるほか、ストレージ システム上でNetAppの数々のテクノロジーと統合されます。Plug-in for IBM Db2 Databaseの操作には、SnapCenterのグラフィカル ユーザ インターフェイスを使用します。

- 統合されたグラフィカルユーザーインターフェース

SnapCenterのインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。どのプラグインでも、SnapCenterのインターフェイスから、バックアップ、リストア、クローニングの各処理を一貫した方法で実行できるほか、ダッシュボード ビューで概要を把握したり、ロールベース アクセス制御（RBAC）を設定したり、ジョブを監視したりすることができます。

- 自動化された中央管理

バックアップ処理のスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理を実行したりできます。SnapCenterからのEメール アラートの送信を設定して、環境をプロアクティブに監視することもできます。

- 無停止の**NetApp**スナップショット コピー テクノロジー

SnapCenterでは、Plug-in for IBM Db2 DatabaseでNetApp Snapshotテクノロジーを使用してリソースがバックアップされます。

Plug-in for IBM Db2を使用すると、次のメリットもあります。

- バックアップ、リストア、およびクローニングのワークフローがサポートされます。
- セキュリティがRBACでサポートされ、ロール委譲が一元化されます。

クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルのアクセス権を付与することもできます。

- NetApp FlexCloneテクノロジーを使用して、テストまたはデータ抽出に使用するリソースのコピー（スペース効率に優れたポイントインタイム コピー）を作成できます。

クローンを作成するストレージ システムにFlexCloneライセンスが必要です。

- バックアップの作成でONTAPの整合グループ（CG）のSnapshot機能がサポートされます。
- 複数のリソース ホストで同時に複数のバックアップを実行できます。

1回の処理で、1つのホストの複数のリソースが同じボリュームを共有する場合に複数のSnapshotが統合されます。

- 外部コマンドを使用してSnapshotを作成できます。
- XFSファイルシステム上のLinux LVMがサポートされます。

SnapCenter Plug-in for IBM Db2でサポートされるストレージ タイプ

SnapCenterは、物理マシンと仮想マシン（VM）の両方でさまざまなストレージ タイプ

をサポートしています。SnapCenter Plug-in for IBM Db2をインストールする前に、ストレージ タイプがサポートされているかどうかを確認する必要があります。

マシン	ストレージ タイプ
物理サーバ	• FC接続LUN • iSCSI接続LUN • NFS接続ボリューム
VMware ESXi	• FCまたはiSCSI HBAで接続されたRDM LUNホスト バス アダプタ (HBA) のスキャンは、SnapCenterがホストに存在するすべてのホスト バス アダプタをスキャンするため、完了までに時間がかかることがあります。 <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> にある LinuxConfig.pm ファイルを編集して、SCSI_HOSTS_OPTIMIZED_RESCAN パラメータの値を 1 に設定し、HBA_DRIVER_NAMES にリストされているHBA のみを再スキャンすることができます。 • iSCSIイニシエータでゲスト システムに直接接続されたiSCSI LUN • NFSデータストア上のVMDK • VMFS上にVMDKが作成されました • ゲスト システムに直接接続されたNFSボリューム • NFSとSANの両方に存在するvVolデータストア vVolデータストアは、ONTAP Tools for VMware vSphereでのみプロビジョニングできます。

IBM Db2プラグインに必要な最小ONTAP権限

必要な最小ONTAP権限は、データ保護に使用するSnapCenterプラグインによって異なります。

- 全アクセス コマンド: ONTAP 9.12.1 以降に必要な最小限の権限
 - event generate-autosupport-log
 - job history show
 - job stop
 - lun

- lun create
- lun create
- lun create
- lun delete
- lun igroup add
- lun igroup create
- lun igroup delete
- lun igroup rename
- lun igroup rename
- lun igroup show
- lun mapping add-reporting-nodes
- lun mapping create
- lun mapping delete
- lun mapping remove-reporting-nodes
- lun mapping show
- lun modify
- lun move-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- lun resize
- lun serial
- lun show
- snapmirror policy add-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- snapmirror restore
- snapmirror show
- snapmirror show-history
- snapmirror update
- snapmirror update-ls-set
- snapmirror list-destinations
- version
- volume clone create
- volume clone show
- volume clone split start

- volume clone split stop
- volume create
- volume destroy
- volume file clone create
- volume file show-disk-usage
- volume offline
- volume online
- volume modify
- volume qtree create
- volume qtree delete
- volume qtree modify
- volume qtree show
- volume restrict
- volume show
- volume snapshot create
- volume snapshot delete
- volume snapshot modify
- volume snapshot modify-snaplock-expiry-time
- volume snapshot rename
- volume snapshot restore
- volume snapshot restore-file
- volume snapshot show
- volume unmount
- vservers cifs
- vservers cifs share create
- vservers cifs share delete
- vservers cifs shadowcopy show
- vservers cifs share show
- vservers cifs show
- vservers export-policy
- vservers export-policy create
- vservers export-policy delete
- vservers export-policy rule create
- vservers export-policy rule show
- vservers export-policy show
- vservers iscsi
- vservers iscsi connection show

- vservers show
- 読み取り専用コマンド: ONTAP 8.3.0以降に必要な最小限の権限
 - ネットワークインターフェース
 - network interface show
 - SVM

IBM Db2でのSnapMirrorレプリケーションとSnapVaultレプリケーションのためのストレージ システムの準備

SnapCenterプラグインと一緒にONTAP SnapMirrorテクノロジーを使用すると、バックアップセットのミラー コピーを別のボリュームに作成できます。また、ONTAP SnapVaultを使用すれば、標準への準拠やその他のガバナンスを目的としたディスクツーディスクのバックアップ レプリケーションを実行できます。これらのタスクを実行する前に、ソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenterは、Snapshot処理の完了後に、SnapMirrorとSnapVaultに対する更新を実行します。SnapMirror更新とSnapVault更新は、SnapCenterジョブの一部として実行されるため、ONTAPスケジュールを別途作成しないでください。



NetApp SnapManager製品からSnapCenterに移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリ ストレージ（ソース ボリューム）上のデータがセカンダリ ストレージ（デスティネーション ボリューム）にレプリケートされます。この関係を初期化すると、ソース ボリュームで参照されるデータ ブロックがデスティネーション ボリュームに転送されます。



SnapCenter は、 SnapMirrorとSnapVaultボリューム間のカスケード関係をサポートしていません (* プライマリ * > ミラー > ボールト)。ファンアウト関係を使用する必要があります。

SnapCenterは、バージョンに依存しないSnapMirror関係の管理をサポートしています。バージョンに依存しないSnapMirror関係とその設定方法の詳細については、["ONTAPのドキュメント"](#)。

IBM Db2のバックアップ戦略

IBM Db2のバックアップ戦略の定義

バックアップ ジョブを作成する前にバックアップ戦略を定義しておく、リソースの正常なリストアやクローニングに必要なバックアップを作成するのに役立ちます。バックアップ戦略の大部分は、サービス レベル アグリーメント（SLA）、目標復旧時間（RTO）、および目標復旧時点（RPO）によって決まります。

タスク概要

SLAとは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。RTOは、サービスの停止からビジネス プロセスの復旧までに必要となる時間です。RPOは、障害発生後に通常処理を再開するためにバックアップ ストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA、RTO、およびRPOは、デー

タ保護戦略に関与します。

手順

1. リソースをバックアップするタイミングを決定します。
2. 必要なバックアップ ジョブの数を決定します。
3. バックアップの命名方法を決定します。
4. Snapshotコピーベースのポリシーを作成してアプリケーションと整合性のあるデータベースのSnapshotをバックアップするかどうかを決定します。
5. レプリケーションのためにNetApp SnapMirrorテクノロジーを使用するか、または長期保持のためにNetApp SnapVaultテクノロジーを使用するかを決定します。
6. ソース ストレージ システムおよびSnapMirrorデスティネーションでのSnapshotの保持期間を確認します。
7. バックアップ処理の前後にコマンドを実行するかどうかを決定し、実行する場合はプリスクリプトまたはポストスクリプトを用意します。

Linuxホスト上のリソースの自動検出

リソースとは、SnapCenterで管理するLinuxホスト上のIBM Db2データベースとインスタンスです。SnapCenter Plug-in for SAP Db2プラグインをインストールすると、そのLinuxホスト上のすべてのインスタンスのIBM Db2データベースが自動的に検出されて[Resources]ページに表示されます。

サポートされるバックアップのタイプ

バックアップ タイプでは、作成するバックアップのタイプを指定します。SnapCenterでは、IBM Db2データベースに対してSnapshotコピーベースのバックアップ タイプがサポートされます。

Snapshotコピーベースのバックアップ

Snapshotコピーベースのバックアップでは、NetApp Snapshotテクノロジーを利用して、IBM Db2データベースが格納されたボリュームのオンラインの読み取り専用のコピーが作成されます。

SnapCenter Plug-in for IBM Db2での整合グループSnapshotの使用方法

プラグインを使用して、リソース グループの整合グループSnapshotを作成することができます。整合グループとはボリュームのコンテナであり、複数のボリュームを格納して1つのエンティティとして管理できます。整合グループには複数のボリュームの同時に作成されたSnapshotが格納されるため、一連のボリュームのコピーの整合性が確保されず。

ストレージ コントローラが整合性を確保しながらSnapshotをグループ化するのを待機する時間も指定できます。利用可能な待機時間のオプションは、「緊急」、「中」、「緩和」です。また、整合グループSnapshotの処理でWrite Anywhere File Layout (WAFL) の同期を有効にするか無効にするかも選択できます。WAFLの同期を有効にすると、整合グループSnapshotのパフォーマンスが向上します。

SnapCenterによる不要なデータ バックアップの削除の管理

SnapCenterは、ストレージ システム レベルおよびファイルシステム レベルで不要なデータバックアップの削除を管理します。

保持設定に基づいて、プライマリ ストレージまたはセカンダリ ストレージのSnapshotが削除され、IBM Db2のカatalog内の対応するエントリも削除されます。

IBM Db2のバックアップ スケジュールを決定する際の考慮事項

バックアップのスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率です。使用頻度の高いリソースは1時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは1日に1回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービス レベル アグリーメント（SLA）、目標復旧時点（RPO）などがあります。

バックアップ スケジュールには、次の2つの要素があります。

- バックアップ頻度（バックアップを実行する間隔）

バックアップ頻度は、ポリシー設定の一部であり、一部のプラグインではスケジュール タイプとも呼ばれます。たとえば、毎時、毎日、毎週、または毎月としてバックアップ頻度を設定できます。

- バックアップ スケジュール（バックアップが実行される日時）

バックアップ スケジュールは、リソースまたはリソース グループの設定の一部です。たとえば、週次バックアップのポリシーが設定されているリソースグループがある場合、毎週木曜日の午後10時にバックアップするようにスケジュールを設定できます。

SAP Db2の必要なバックアップ ジョブの数

必要なバックアップ ジョブの数を左右する要因としては、リソースのサイズ、使用中のボリュームの数、リソースの変更率、サービス レベル アグリーメント（SLA）などがあります。

Plug-in for IBM Db2データベースのバックアップの命名規則

Snapshotのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則ではSnapshot名にタイムスタンプが追加されるので、コピーが作成されたタイミングを特定できます。

Snapshotでは、次のデフォルトの命名規則が使用されます。

resourcegroupname_hostname_timestamp

バックアップ リソース グループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- *dts1* はリソース グループ名です。
- *mach1x88* はホスト名です。
- *03-12-2015_23.17.26* は日付とタイムスタンプです。

または、[スナップショット コピーにカスタム名形式を使用する] を選択して、リソースまたはリソース グループを保護しながらスナップショット名の形式を指定することもできます。たとえば、*customtext_resourcegroup_policy_hostname*や*resourcegroup_hostname*などの形式です。デフォルトでは、Snapshot名にタイムスタンプのサフィックスが追加されます。

IBM Db2のリストアとリカバリの戦略

IBM Db2リソースのリストアとリカバリの戦略の定義

データベースのリストアとリカバリを行う前に戦略を定義しておく、リストア処理とリカバリ処理を正常に実行できるようになります。



データベースの手動リカバリのみがサポートされます。

手順

1. 手動で追加したIBM Db2リソースでサポートされるリストア戦略を確認します。
2. 自動検出されたIBM Db2データベースでサポートされるリストア戦略を確認します。

手動で追加した**IBM Db2**リソースでサポートされるリストア戦略のタイプ

SnapCenterを使用してリストア処理を正常に実行するには、戦略を定義しておく必要があります。手動で追加したIBM Db2リソースには、2種類のリストア戦略があります。



手動で追加したIBM Db2リソースはリカバリできません。

リソース全体のリストア

- リソースのすべてのボリューム、qtree、およびLUNをリストア



リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeのリストア用のSnapshotが選択されたあとに作成されたSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。

自動検出された**IBM Db2**でサポートされるリストア戦略のタイプ

SnapCenterを使用してリストア処理を正常に実行するには、戦略を定義しておく必要があります。

リソースの完全なリストアは、自動検出されたIBM Db2データベースに対してサポートされているリストア戦略です。この戦略では、リソースのすべてのボリューム、qtree、およびLUNがリストアされます。

自動検出された**IBM Db2**のリストア処理のタイプ

SnapCenter Plug-in for IBM Db2では、自動検出されたIBM Db2データベースに対して、Single File SnapRestoreおよびConnect and Copyのリストア タイプがサポートされます。

NFS環境でSingle File SnapRestoreを実行するシナリオは、次のとおりです。

- *完全なリソース*オプションのみを選択した場合
- 選択したバックアップがSnapMirrorまたはSnapVaultのセカンダリロケーションからのものであり、*完全なリソース*オプションが選択されている場合

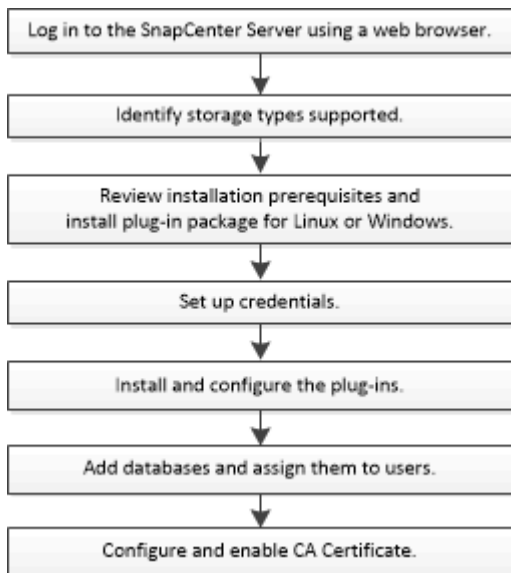
SAN環境でSingle File SnapRestoreを実行するシナリオは、次のとおりです。

- *完全なリソース*オプションのみを選択した場合
- バックアップがSnapMirrorまたはSnapVaultのセカンダリロケーションから選択され、*完全なリソース*オプションが選択されている場合

SnapCenter Plug-in for IBM Db2のインストール準備

SnapCenter Plug-in for IBM Db2のインストール ワークフロー

IBM Db2データベースを保護する場合は、SnapCenter Plug-in for IBM Db2をインストールしてセットアップする必要があります。



Windows、Linux、または AIX 用のホストを追加し、プラグイン パッケージをインストールするための前提条件

ホストを追加してプラグイン パッケージをインストールする前に、すべての要件を満たしておく必要があります。Windows、Linux、AIX 環境でサポートされる IBM Db2 用のSnapCenterプラグイン。

- Java 11をホストにインストールしておく必要があります。



IBM Java は Windows および Linux ホストではサポートされていません。

- Windows の場合、プラグイン クリエーター サービスは、“LocalSystem” Windows ユーザーを使用して実行する必要があります。これは、IBM Db2 用プラグインがドメイン管理者としてインストールされている場合のデフォルトの動作です。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。WindowsホストにIBM Db2プラグインをインストールすると、SnapCenter Plug-in for Microsoft Windowsもデフォルトで導入されます。
- SnapCenter Serverが、Plug-in for IBM Db2ホストの8145ポートまたはカスタム ポートにアクセスできる必要があります。

Windowsホスト

- ローカル管理者権限があり、リモート ホストに対してローカル ログインのアクセス許可があるドメイン ユーザが必要です。
- Plug-in for IBM Db2をWindowsホストにインストールすると、SnapCenter Plug-in for Microsoft Windows が自動的にインストールされます。
- rootユーザまたはroot以外のユーザに対してパスワード ベースのSSH接続を有効にしておく必要があります。
- Java 11をWindowsホストにインストールしておく必要があります。

["Windows用JAVAをダウンロード"](#)

["NetApp Interoperability Matrix Tool"](#)

LinuxおよびAIXホスト

- rootユーザまたはroot以外のユーザに対してパスワード ベースのSSH接続を有効にしておく必要があります。
- Java 11をLinuxホストにインストールしておく必要があります。

["Linux用JAVAをダウンロード"](#)

["AIX用JAVAをダウンロード"](#)

["NetApp Interoperability Matrix Tool"](#)

- LinuxホストでIBM Db2データベースを実行している場合は、Plug-in for IBM Db2のインストール時にSnapCenter Plug-in for UNIXが自動的にインストールされます。
- プラグインのインストールには、デフォルトのシェルとして **bash** を使用する必要があります。

補助コマンド

SnapCenterプラグイン for IBM Db2 で補足コマンドを実行するには、そのコマンドを *allowed_commands.config* ファイルに含める必要があります。

- Windows ホスト上のデフォルトの場所: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux ホスト上のデフォルトの場所: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`

プラグイン ホストで補足コマンドを許可するには、エディターで `allowed_commands.config` ファイルを開きます。各コマンドを別々の行に入力します。コマンドでは大文字と小文字は区別されません。完全修飾パス名を指定し、パス名にスペースが含まれている場合は引用符 (") で囲んでください。

例えば：

command: mount

command: umount

コマンド: "C:\Program Files\NetApp\SnapCreator コマンド\sdcli.exe"

command: myscript.bat

`allowed_commands.config` ファイルが存在しない場合、コマンドまたはスクリプトの実行はブロックされ、ワークフローは次のエラーで失敗します。

"[/mnt/mount -a] の実行は許可されていません。Authorize by adding the command in the file %s on the plugin host."

コマンドまたはスクリプトが `allowed_commands.config` に存在しない場合、コマンドまたはスクリプトの実行はブロックされ、ワークフローは次のエラーで失敗します。

"[/mnt/mount -a] の実行は許可されていません。Authorize by adding the command in the file %s on the plugin host."



すべてのコマンドを許可するには、ワイルドカード エントリ (*) を使用しないでください。

Linuxホストのroot以外のユーザへのsudo権限の設定

SnapCenter、非ルート ユーザーが Linux 用のSnapCenterプラグイン パッケージをインストールし、プラグイン プロセスを開始できます。プラグイン プロセスは有効なroot以外のユーザとして実行されます。いくつかのパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

必要なもの

- sudoバージョン1.8.7以降
- umask が 0027 の場合、java フォルダーとその中のすべてのファイルに 555 の権限があることを確認します。そうしないと、プラグインのインストールが失敗する可能性があります。
- root以外のユーザについては、root以外のユーザの名前とユーザのグループが同じであることを確認してください。
- `/etc/ssh/sshd_config` ファイルを編集して、メッセージ認証コード アルゴリズム (MAC hmac-sha2-256 および MAC hmac-sha2-512) を設定します。

この構成ファイルを更新したら、sshdサービスを再起動します。

例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

このタスクについて

次のパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /custom_location/NetApp/snapcenter/spl/bin/spl

手順

1. SnapCenter Plug-ins Package for LinuxをインストールするLinuxホストにログインします。
2. visudo Linuxユーティリティを使用して、/etc/sudoersファイルに次の行を追加します。

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```



RAC をセットアップしている場合は、他の許可されたコマンドとともに、`/etc/sudoers` ファイルに次の行を追加する必要があります: `'/<crs_home>/bin/olsnodes'`

`crs_home` の値は、`/etc/oracle/olr.loc` ファイルから取得できます。

`LINUX_USER` は、作成した非 root ユーザーの名前です。

`checksum_value` は、次の場所にある `sc_unix_plugins_checksum.txt` ファイルから取得できます。

- SnapCenter Server が Windows ホストにインストールされている場合は、`C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`。
- SnapCenter Server が Linux ホストにインストールされている場合は、`/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`。



この例は、独自のデータを作成する際の参照としてのみ使用してください。

AIXホストのroot以外のユーザへのsudo権限の設定

SnapCenter 4.4以降では、root以外のユーザがSnapCenter Plug-ins Package for AIXをインストールしてプラグイン プロセスを開始できます。プラグイン プロセスは有効なroot以外のユーザとして実行されます。いくつかのパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

必要なもの

- sudoバージョン1.8.7以降
- umask が 0027 の場合、java フォルダーとその中のすべてのファイルに 555 の権限があることを確認します。そうしないと、プラグインのインストールが失敗する可能性があります。
- `/etc/ssh/sshd_config` ファイルを編集して、メッセージ認証コード アルゴリズム (MAC hmac-sha2-256 および MAC hmac-sha2-512) を設定します。

この構成ファイルを更新したら、sshdサービスを再起動します。

例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

このタスクについて

次のパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

- /home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /custom_location/NetApp/snapcenter/spl/bin/spl

手順

1. SnapCenter Plug-ins Package for AIXをインストールするAIXホストにログインします。
2. visudo Linuxユーティリティを使用して、/etc/sudoersファイルに次の行を追加します。

```
Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```



RAC をセットアップしている場合は、他の許可されたコマンドとともに、/etc/sudoers ファイルに次の行を追加する必要があります: '/<crs_home>/bin/olsnodes'

crs_home の値は、*/etc/oracle/olr.loc* ファイルから取得できます。

AIX_USER は、作成した非 root ユーザーの名前です。

checksum_value は、次の場所にある **sc_unix_plugins_checksum.txt** ファイルから取得できます。

- SnapCenter Server が Windows ホストにインストールされている場合は、*C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt*。
- SnapCenter Server が Linux ホストにインストールされている場合は、*/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt*。



この例は、独自のデータを作成する際の参照としてのみ使用してください。

SnapCenter Plug-ins Package for Windowsをインストールするホストの要件

SnapCenter Plug-ins Package for Windowsをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	Microsoft Windows サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	5 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。

SnapCenter Plug-ins Package for Linuxをインストールするホストの要件

SnapCenter Plug-ins Package for Linuxをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。

項目	要件
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	2 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエントリの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	Java 11 Oracle JavaおよびOpenJDK Javaを最新バージョンにアップグレードした場合は、<code>/var/opt/snapcenter/spl/etc/spl.properties</code>にある<code>JAVA_HOME</code>オプションが正しいJavaバージョンと正しいパスに設定されていることを確認する必要があります。 サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。

SnapCenter Plug-in for IBM Db2のクレデンシャルの設定

SnapCenterは、クレデンシャルを使用してSnapCenterの処理を実行するユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、データベースやWindowsファイルシステムでのデータ保護処理に使用するクレデンシャルをそれぞれ作成する必要があります。

タスク概要

- Linuxホスト

Linuxホストにプラグインをインストールするには、クレデンシャルを設定する必要があります。

このクレデンシャルは、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo権限があるroot以外のユーザに対して設定します。

ベスト プラクティス: ホストをデプロイしてプラグインをインストールした後でも Linux の認証情報を作成できますが、ベスト プラクティスとしては、SVM を追加した後、ホストをデプロイしてプラグインをインストールする前に認証情報を作成します。

- Windowsホスト

プラグインのインストール前にWindowsクレデンシャルを設定する必要があります。

このクレデンシャルには、管理者権限（リモート ホストに対する管理者権限を含む）を設定する必要があります。

個々のリソース グループのクレデンシャルを設定する場合で、ユーザ名に完全なadmin権限が割り当てられていない場合は、少なくともリソース グループとバックアップの権限を割り当てる必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定] ページで、[資格情報] をクリックします。
3. *新規* をクリックします。
4. [Credential] ページで、クレデンシャルの設定に必要な情報を指定します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。
ユーザ名	認証に使用するユーザ名とパスワードを入力します。 • ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者またはSnapCenterプラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。ユーザ名フィールドの有効な形式は次のとおりです。 ◦ <i>NetBIOS</i>\ユーザー名 ◦ ドメイン<i>FQDN</i>\ユーザー名 • ローカル管理者（ワークグループの場合のみ） ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。ユーザー名フィールドの有効な形式は次のとおりです: <i>UserName</i> パスワードには二重引用符 (") やバッククォート (`) を使用しないでください。未満記号 (<) と感嘆符 (!) を組み合わせて使用したりしないでください。たとえば、lessthan<!10、lessthan10<!、バックティック `12 などです。

フィールド	操作
パスワード	認証に使用するパスワードを入力します。
Authentication Mode	使用する認証モードを選択します。
Use sudo privileges	非 root ユーザーの資格情報を作成する場合は、[sudo 権限を使用する] チェックボックスをオンにします。  Linuxユーザのみに該当します。

5. [OK]をクリックします。

クレデンシャルの設定が完了したら、必要に応じて[User and Access]ページでユーザやユーザ グループにクレデンシャルを割り当てることができます。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、作成したグループ管理サービス アカウント (gMSA) を通じて、管理対象ドメイン アカウントからサービス アカウントのパスワードを自動管理できます。

開始する前に

- Windows Server 2016以降のドメイン コントローラが必要です。
- ドメインのメンバーであるWindows Server 2016以降のホストが必要です。

手順

1. KDSルート キーを作成し、gMSA内のオブジェクトごとに一意のパスワードを生成します。
2. 各ドメインについて、Windowsドメインコントローラから次のコマンドを実行します: Add-KDSRootKey -Effectivelmmediately
3. gMSAを作成して設定します。
 - a. 次の形式でユーザ グループ アカウントを作成します。

```
domainName\accountName$
.. コンピュータ オブジェクトをグループに追加します。
.. 作成したユーザ グループを使用してgMSAを作成します。
```

次に例を示します。


```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. 走る `Get-ADServiceAccount` サービス アカウントを確認するコマンド。
```

4. ホストでgMSAを設定します。

- a. gMSAアカウントを使用するホストで、Windows PowerShell用のActive Directoryモジュールを有効にします。

これを行うには、PowerShellから次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. ホストを再起動します。
 - b. PowerShell コマンド プロンプトから次のコマンドを実行して、ホストに gMSA をインストールします。 `Install-AdServiceAccount <gMSA>`
 - c. 次のコマンドを実行して、gMSA アカウントを確認します。 `Test-AdServiceAccount <gMSA>`
5. ホスト上の設定済みgMSAに管理者権限を割り当てます。
 6. SnapCenter Serverで設定済みのgMSAアカウントを指定してWindowsホストを追加します。

SnapCenter Serverにより、選択したプラグインがホストにインストールされ、プラグインのインストール時には指定したgMSAがサービスのログオン アカウントとして使用されます。

SnapCenter Plug-in for IBM Db2のインストール

SnapCenterの[Add Host]ページを使用してホストを追加し、プラグイン パッケージをインストールする必要があります。プラグインは、自動的にリモート ホストにインストールされます。ホストの追加とプラグイン パッケージのインストールは、ホストごとまたはクラスタごとに実行できます。

開始する前に

- SnapCenter Serverホストのオペレーティング システムがWindows 2019で、プラグイン ホストのオペレーティング システムがWindows 2022の場合は、次の手順を実行する必要があります。
 - Windows Server 2019 (OSビルド17763.5936) 以降にアップグレードする
 - Windows Server 2022 (OSビルド20348.2402) 以降にアップグレードする
- この処理は、SnapCenter Adminロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。
- メッセージ キュー サービスが実行中であることを確認する必要があります。
- ホストの管理については、管理に関するドキュメントを参照してください。
- グループ管理サービス アカウント (gMSA) を使用する場合は、管理者権限でgMSAを設定する必要があります。

["Windows Server 2016 以降で IBM Db2 用のグループ管理サービス アカウントを構成する"](#)

タスク概要

- SnapCenter Serverをプラグイン ホストとして別のSnapCenter Serverに追加することはできません。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. 上部の*管理対象ホスト*タブが選択されていることを確認します。
3. *[追加]*をクリックします。
4. [Hosts]ページで、次の操作を実行します。

フィールド	操作
ホストタイプ	ホストのタイプを選択します。 • Windows • Linux  Plug-in for IBM Db2は、IBM Db2 クライアント ホストにインストールされます。このホストは、WindowsシステムでもLinuxシステムでもかまいません。
ホスト名	通信ホスト名を入力します。ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。SnapCenterが機能するためには、DNSが適切に設定されている必要があります。そのため、FQDNを入力することを推奨します。
Credentials	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。このクレデンシャルには、リモート ホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。  クレデンシャルの認証モードは、[Add Host]ウィザードで指定するホスト タイプによって決まります。

5. [Select Plug-ins to Install]セクションで、インストールするプラグインを選択します。

REST APIを使用してPlug-in for Db2をインストールする場合は、バージョンを3.0として渡す必要があります。例：Db2:3.0

6. (オプション) [その他のオプション] をクリックします。

フィールド	操作
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。デフォルトのポート番号は8145です。SnapCenter Serverがカスタム ポートにインストールされている場合は、そのポート番号がデフォルト ポートとして表示されます。  プラグインを手動でインストールしてカスタム ポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理が失敗します。
Installation Path	Plug-in for IBM Db2は、IBM Db2クライアント ホストにインストールされます。このホストは、WindowsシステムでもLinuxシステムでもかまいません。 • Windows 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは C:\Program Files\ NetApp\ SnapCenterです。必要に応じて、パスをカスタマイズできます。 • Linux 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは /opt/ NetApp/snapcenter です。必要に応じて、パスをカスタマイズできます。
Skip preinstall checks	プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスをオンにします。
Use group Managed Service Account (gMSA) to run the plug-in services	Windowsホストで、グループ管理サービス アカウント (gMSA) を使用してプラグイン サービスを実行する場合は、このチェック ボックスをオンにします。  gMSA名をdomainName\accountName\$の形式で指定します。  gMSAは、SnapCenter Plug-in for Windowsサービスのログオン サービス アカウントとしてのみ使用されます。

7. *送信*をクリックします。

[Skip prechecks]チェック ボックスを選択していない場合、プラグインをインストールするための要件をホストが満たしているかどうかを検証するためにホストが検証されます。ディスク スペース、RAM、PowerShellのバージョン、.NETのバージョン、場所（Windowsプラグインの場合）、Java 11（WindowsプラグインとLinuxプラグインの場合）が最小要件に照らして検証されます。最小要件を満たしていない場合、対応するエラーまたは警告メッセージが表示されます。

エラーがディスク スペースまたはRAMに関連している場合は、C:\Program Files\NetApp\SnapCenter WebAppにあるweb.configファイルを更新してデフォルト値を変更できます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。



HAのセットアップでweb.configファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. ホスト タイプが Linux の場合は、フィンガープリントを確認し、[確認して送信] をクリックします。

クラスタ セットアップでは、クラスタ内の各ノードのフィンガープリントを検証する必要があります。



前述の手順で同じホストがSnapCenterに追加され、フィンガープリントが確認された場合でも、フィンガープリントの検証は必須です。

9. インストールの進捗状況を監視します。

- Windows プラグインの場合、インストール ログとアップグレード ログは次の場所にあります：
C:\Windows\SnapCenter plugin\Install<JOBID>\
- Linux プラグインの場合、インストール ログは次の場所にあります：
/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log、アップグレード ログは次の場所にあります：/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log

終了後の操作

SnapCenter 6.0 以降にアップグレードする場合、既存の PERL ベースの Db2 用プラグインはリモート プラグイン サーバーからアンインストールされます。

コマンドレットを使用した複数のリモート ホストへの**SnapCenter Plug-ins Package for Linux / Windows**のインストール

Install-SmHostPackage PowerShellコマンドレットを使用すると、複数のホストにSnapCenter Plug-ins Package for Linux / Windowsを同時にインストールできます。

開始する前に

プラグイン パッケージをインストールする各ホストに対するローカル管理者権限を持つドメイン ユーザとして、SnapCenterにログインしておく必要があります。

手順

1. PowerShellを起動します。
2. SnapCenter Serverホストで、Open-SmConnectionコマンドレットを使用してセッションを確立し、クレデンシャルを入力します。
3. Install-SmHostPackageコマンドレットと必要なパラメータを使用して、複数のホストにプラグインをインストールします。

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行す

ると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、-skipprecheckオプションを使用できます。

4. リモート インストールのクレデンシャルを入力します。

コマンドライン インターフェイスを使用したLinuxホストへの**SnapCenter Plug-in for IBM Db2**のインストール

SnapCenter Plug-in for IBM Db2 Databaseは、SnapCenterユーザ インターフェイス (UI) を使用してインストールする必要があります。SnapCenter UIからのプラグインのリモート インストールが許可されていない環境では、コマンドライン インターフェイス (CLI) を使用して、コンソール モードまたはサイレント モードでPlug-in for IBM Db2 Databaseをインストールできます。

開始する前に

- Plug-in for IBM Db2 Databaseは、IBM Db2クライアントがあるLinuxホストごとにインストールする必要があります。
- SnapCenter Plug-in for IBM Db2 DatabaseをインストールするLinuxホストは、依存するソフトウェア、データベース、オペレーティング システムの要件を満たしている必要があります。

サポートされる構成に関する最新の情報については、Interoperability Matrix Tool (IMT) を参照してください。

["NetApp Interoperability Matrix Tool"](#)

- SnapCenter Plug-in for IBM Db2 Databaseは、SnapCenter Plug-ins Package for Linuxに含まれています。SnapCenter Plug-ins Package for Linuxをインストールする前に、SnapCenterをWindowsホストにインストールしておく必要があります。

タスク概要

パラメータが指定されていない場合、SnapCenterはデフォルト値でインストールされます。

手順

1. SnapCenter Plug-ins Package for Linuxのインストール ファイル (snapcenter_linux_host_plugin.bin) をC:\ProgramData\NetApp\SnapCenter\Package RepositoryからPlug-in for IBM Db2をインストールするホストにコピーします。

このパスには、SnapCenter Serverがインストールされているホストからアクセスできます。

2. コマンド プロンプトから、インストール ファイルをコピーしたディレクトリに移動します。
3. プラグインをインストールします。

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address  
-DSERVER_HTTPS_PORT=port_number_for_server
```

- -DPORT は SMCORE HTTPS 通信ポートを指定します。
- -DSERVER_IP は、 SnapCenter Server の IP アドレスを指定します。

- -DSEVER_HTTPS_PORT は、 SnapCenter Server の HTTPS ポートを指定します。
- -DUSER_INSTALL_DIR は、 Linux 用の SnapCenter プラグイン パッケージをインストールするディレクトリを指定します。
- DINSTALL_LOG_NAME はログ ファイルの名前を指定します。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSEVER_IP=scserver.domain.com -DSEVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. /<インストール ディレクトリ>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties ファイルを編集し、 PLUGINS_ENABLED = DB2:3.0 パラメータを追加します。
5. Add-Smhost コマンドレットと必要なパラメータを使用して、 SnapCenter Server にホストを追加します。

コマンドで利用できるパラメータとその説明に関する情報は、 *Get-Help command_name* を実行すると取得できます。あるいは、 "[SnapCenter ソフトウェア コマンドレット リファレンス ガイド](#)"。

Plug-in for IBM Db2 のインストール ステータスの監視

[Jobs] ページを使用して、 SnapCenter プラグイン パッケージのインストールの進捗状況を監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs] ページでは、 次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、 警告のため開始できませんでした
-  キューに登録

手順

1. 左側のナビゲーション ペインで、 [モニター] をクリックします。
2. *モニター* ページで、 *ジョブ* をクリックします。
3. ジョブ ページで、 プラグインのインストール操作のみがリストされるようにリストをフィルタリングするには、 次の手順を実行します。
 - a. *フィルター* をクリックします。
 - b. オプション： 開始日と終了日を指定します。
 - c. [タイプ] ドロップダウン メニューから、 [プラグインのインストール] を選択します。

- d. [Status]ドロップダウン メニューから、インストールのステータスを選択します。
- e. *適用*をクリックします。
4. インストール ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

CA証明書の設定

CA証明書CSRファイルの生成

証明書署名要求（CSR）を生成し、生成したCSRを使用して認証局（CA）から取得した証明書をインポートできます。証明書には秘密キーが関連付けられます。

CSRはエンコードされたテキストのブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。



CA 証明書の RSA キーの長さは最低 3072 ビットである必要があります。

CSRを生成するための情報については、["CA証明書CSRファイルの生成方法"](#)。



ドメイン (*.domain.company.com) またはシステム (machine1.domain.company.com) の CA 証明書を所有している場合は、CA 証明書 CSR ファイルの生成をスキップできます。SnapCenterを使用して、既存のCA証明書を導入できます。

クラスタ構成の場合、クラスタ名（仮想クラスタFQDN）と、それぞれのホスト名がCA証明書に記載されている必要があります。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。ワイルドカード証明書 (*.domain.company.com) の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenter ServerとWindowsホスト プラグインにCA証明書をインポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
4. コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書 をクリックします。
5. 「信頼されたルート証明機関」フォルダを右クリックし、[すべてのタスク] > [インポート] を選択して、インポート ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*次へ*をクリックします。
インポート ファイル形式	変更せずに、[次へ] をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、[次へ] をクリックします。
証明書のインポート ウィザードの完了	概要を確認し、[完了] をクリックしてインポートを開始します。



インポートする証明書は秘密キーとバンドルされている必要があります (サポートされている形式は **.pfx**、**.p12**、および ***.p7b** です)。

7. 「個人用」フォルダに対して手順5を繰り返します。

CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための16進数の文字列です。サムプリントは、サムプリント アルゴリズムを使用して証明書の内容から計算されます。

手順

1. GUIで次の手順を実行します。

- a. 証明書をダブルクリックします。
- b. [証明書] ダイアログボックスで、[詳細] タブをクリックします。
- c. フィールドのリストをスクロールして、「拇印」をクリックします。
- d. ボックスから16進数の文字をコピーします。
- e. 16進数の間のスペースを削除します。

たとえば、拇印が「a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b」の場合、スペースを削除すると「a909502dd82ae41433e6f83886b00d4277a32a7b」になります。

2. PowerShellで、次の手順を実行します。

- a. 次のコマンドを実行して、インストールされている証明書のサムプリントを表示し、最近インストールされた証明書をサブジェクト名で識別します。

```
Get-ChildItem -Path 証明書:\LocalMachine\My
```

- b. サムプリントをコピーします。

Windowsホスト プラグイン サービスでのCA証明書の設定

インストールされているデジタル証明書をアクティブ化するには、Windowsホスト プラ

グイン サービスを使用してCA証明書を設定する必要があります。

SnapCenter Serverと、CA証明書がすでに導入されているすべてのプラグイン ホストで、次の手順を実行します。

手順

1. 次のコマンドを実行して、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例えば：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 次のコマンドを実行して、新しくインストールした証明書をWindowsホスト プラグイン
サービスとバインドします。
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例えば：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

LinuxホストでのSnapCenter IBM Db2プラグイン サービスのCA証明書の設定

インストールされたデジタル証明書をアクティブ化するには、SnapCenterプラグイン サービスを使用して、プラグイン キーストアとその証明書のパスワードを管理し、CA 証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成 し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、`/opt/NetApp/snapcenter/scc/etc`にあるファイル「`keystore.jks`」を使用します。

プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

キー「`KEYSTORE_PASS`」に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```

・ キーストア内の秘密キー
エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

agent.properties ファイルのキー `KEYSTORE_PASS` も同様に更新します。

3. パスワードを変更したら、サービスを再起動します。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは同じである必要があります。

ルート証明書または中間証明書をプラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグイン キーストアが含まれるフォルダーに移動します: `/opt/ NetApp/snapcenter/scc/etc`。
2. 「`keystore.jks`」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. ルート証明書か中間証明書を追加します。

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

・ ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアに**CA**署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグイン キーストア `/opt/ NetApp/snapcenter/scc/etc` が含まれるフォルダーに移動します。

2. 「keystore.jks」ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

6. キーストアに追加された新しいCA証明書に対応するエイリアスが、キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのプラグイン キーストア パスワードは、agent.properties ファイルのキー KEYSTORE_PASS の値です。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

・ CA 証明書のエイリアス名が長く、スペースや特殊文字（「*」、「」）が含まれている場合は、エイリアス名を単純な名前に変更します。

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

・ agent.properties ファイルのCA証明書からエイリアス名を設定します。

この値を、キーSCC_CERTIFICATE_ALIASに対して更新します。

8. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

プラグインの証明書失効リスト（CRL）を構成する

タスク概要

- ・ SnapCenterプラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- ・ SnapCenterプラグインの CRL ファイルのデフォルト ディレクトリは、「opt/NetApp/snapcenter/scc/etc/crl」です。

手順

1. キーCRL_PATHに対して、agent.propertiesファイルのデフォルト ディレクトリを変更、更新できます。

このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

WindowsホストでのSnapCenter IBM Db2プラグイン サービスのCA証明書の設定

インストールされたデジタル証明書をアクティブ化するには、SnapCenterプラグインサービスを使用して、プラグイン キーストアとその証明書のパスワードを管理し、CA証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、`C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc`にあるファイル `keystore.jks` を使用します。

プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

これはキー `_KEYSTORE_PASS_` に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```



Windowsコマンド プロンプトで「keytool」 コマンドが認識されない場合は、keytoolコマンドを完全なパスに置き換えます。

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. キーストア内の秘密キー エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

```
keytool -keypasswd -alias "証明書内のエイリアス名" -keystore keystore.jks
```

`agent.properties` ファイルのキー `KEYSTORE_PASS` も同様に更新します。

4. パスワードを変更したら、サービスを再起動します。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは同じである必要があります。

ルート証明書または中間証明書をプラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc` に移動します。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. ルート証明書か中間証明書を追加します。

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアにCA署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `_C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc_` に移動します。
2. ファイル `keystore.jks` を見つけます。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

6. キーストアに追加された新しいCA証明書に対応するエイリアスが、キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのプラグイン キーストア パスワードは、`agent.properties` ファイルのキー `KEYSTORE_PASS` の値です。

```
keytool -keypasswd -alias "CA証明書のエイリアス名" -keystore keystore.jks
```

8. `agent.properties` ファイル内の CA 証明書からエイリアス名を設定します。

この値を、キー `SCC_CERTIFICATE_ALIAS` に対して更新します。

9. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

SnapCenter プラグインの証明書失効リスト (CRL) を構成する

タスク概要

- 関連するCA証明書の最新のCRLファイルをダウンロードするには、["SnapCenter CA証明書の証明書失効リストファイルを更新する方法"](#)。

- SnapCenterプラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- SnapCenterプラグインの CRL ファイルのデフォルト ディレクトリは、'`C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\crl`' です。

手順

1. キー `CRL_PATH` に対して、`agent.properties` ファイル内のデフォルト ディレクトリを変更および更新できます。
2. このディレクトリには、複数のCRLファイルを格納できます。

受信する証明書については、それぞれのCRLに対して検証が行われます。

プラグインのCA証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインでCA証明書の検証を有効にする必要があります。

開始する前に

- 実行 `Set-SmCertificateSettings` コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- `Get-SmCertificateSettings` を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. プラグイン ホストを1つまたは複数選択します。
4. *その他のオプション*をクリックします。
5. *証明書の検証を有効にする*を選択します。

終了後の操作

[Managed Hosts]タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Serverとプラグイン ホスト間の接続のステータスを示します。

- *  * は、CA 証明書が有効になっていないか、プラグイン ホストに割り当てられていないことを示します。
- *  * は CA 証明書が正常に検証されたことを示します。
- *  * は、CA 証明書を検証できなかったことを示します。
- *  * は接続情報を取得できなかったことを示します。



ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

データ保護の準備

SnapCenter Plug-in for IBM Db2を使用するための前提条件

ユーザがSnapCenter Plug-in for IBM Db2を使用するためには、SnapCenter管理者が事前にSnapCenter Serverをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter Serverをインストールして設定します。
- SnapCenter Serverにログインします。
- SnapCenter環境を設定するために、必要に応じて、ストレージ システム接続を追加し、クレデンシャルを作成します。
- LinuxホストまたはWindowsホストにJava 11をインストールします。

Javaパスは、ホスト マシンの環境パス変数で設定する必要があります。

- バックアップ レプリケーションが必要である場合は、SnapMirrorとSnapVaultをセットアップします。

IBM Db2の保護におけるリソース、リソース グループ、ポリシーの使用方法

SnapCenterを使用する前に、実行するバックアップ、クローニング、リストアの各処理に関連する基本的な概念を理解しておく役立ちます。ここでは、これらの処理で扱うリソース、リソース グループ、およびポリシーについて説明します。

- リソースとは、一般にはSnapCenterでバックアップまたはクローニングするIBM Db2データベースのことです。
- SnapCenterリソース グループは、ホスト上のリソースの集まりです。

リソース グループに対して処理を実行すると、リソース グループに指定したスケジュールに従って、リソース グループに定義されているリソースに対して処理が実行されます。

単一のリソースまたはリソース グループをオンデマンドでバックアップすることができます。また、スケジュールされたバックアップを単一リソースおよびリソース グループに対して実行することもできます。

- ポリシーは、バックアップ頻度、レプリケーション、スクリプトといった、データ保護処理の特性を指定するものです。

リソース グループを作成するときに、そのグループに対して1つ以上のポリシーを選択します。単一リソースに対してオンデマンドでバックアップを実行するときにもポリシーを選択できます。

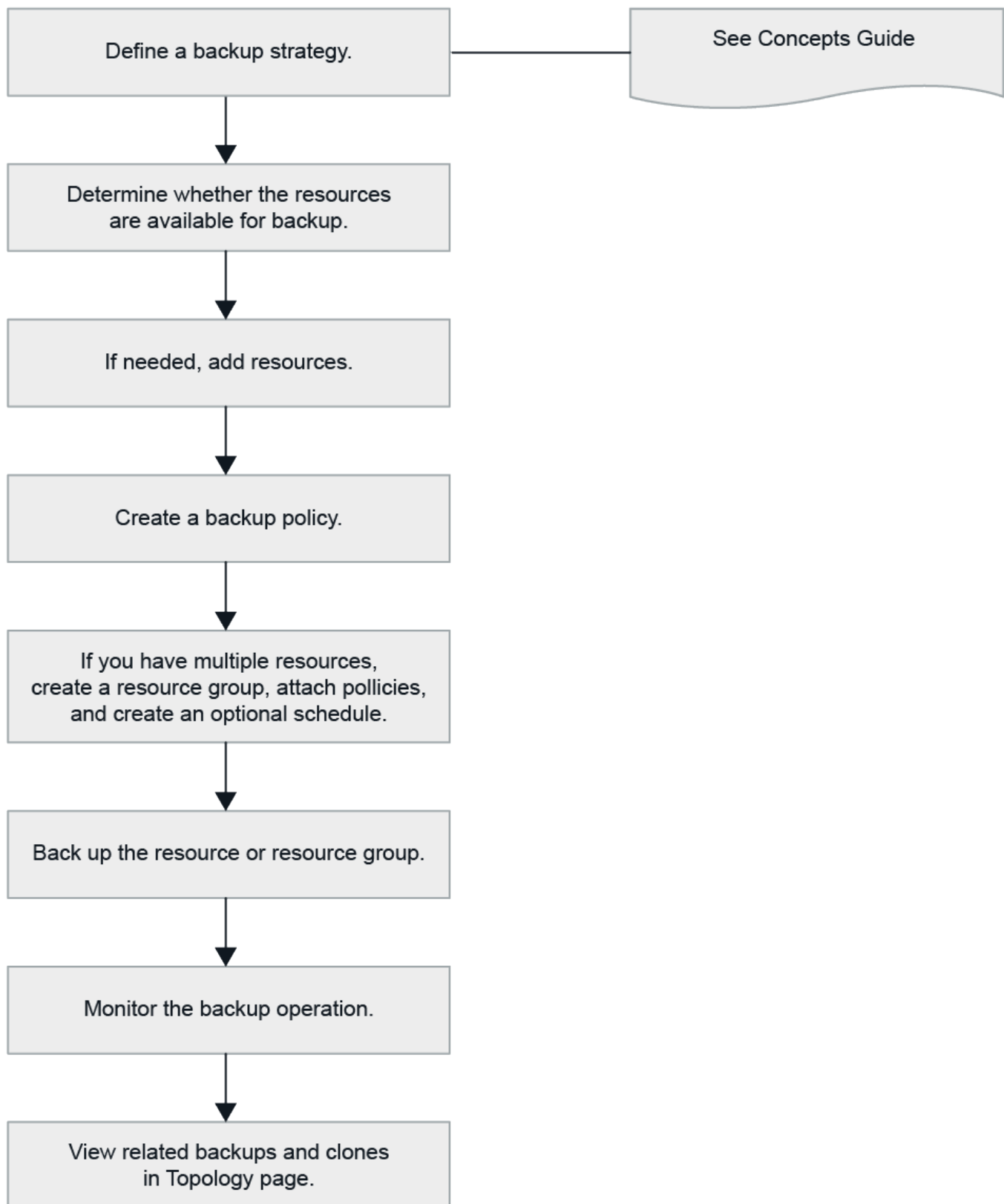
リソース グループでは、保護する対象と保護するタイミング（日時）を定義できます。ポリシーでは、保護する方法を定義できます。たとえば、すべてのデータベースをバックアップする場合は、ホストのすべてのデータベースを含むリソース グループを作成します。このリソース グループに、日次ポリシーと毎時ポリシーの2つのポリシーを適用します。リソース グループを作成してポリシーを適用する際に、フル バックアップを1日1回実行するようにリソース グループを設定できます。

IBM Db2リソースのバックアップ

IBM Db2リソースのバックアップ

リソース（データベース）またはリソース グループのバックアップを作成することができます。バックアップのワークフローには、計画、バックアップするデータベースの特定、バックアップ ポリシーの管理、リソース グループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

次のワークフローは、バックアップ処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトでを使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。<https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html>["SnapCenterソフトウェア コマンドレット リファレンス ガイド"^]。

データベースの自動的検出

リソースとなるのは、ホスト上でSnapCenterによって管理されているLinuxホスト上のIBM Db2データベースです。使用できるIBM Db2データベースを検出したあとに、それらのリソースをリソース グループに追加してデータ保護処理を実行できます。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の作成などのタスクを事前に完了しておく必要があります。
- SnapCenter Plug-in for IBM Db2では、RDM / VMDK仮想環境にあるリソースの自動検出がサポートされていません。データベースを手動で追加する際に、仮想環境のストレージの情報を指定する必要があります。

タスク概要

- プラグインをインストールすると、そのLinuxホスト上のすべてのデータベースが自動検出されて[Resources]ページに表示されます。
- 自動検出されるのはデータベースだけです。

自動検出されたリソースを変更または削除することはできません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから [IBM Db2 用プラグイン] を選択します。
2. [Resources]ページで、[View]リストからリソース タイプを選択します。
3. (オプション) をクリック 、ホスト名を選択します。
をクリックします  フィルター パネルを閉じます。
4. ホスト上で利用可能なリソースを検出するには、[リソースの更新] をクリックします。

リソースは、リソース タイプ、ホスト名、関連するリソース グループ、バックアップ タイプ、ポリシー、全体的なステータスなどの情報とともに表示されます。

- データベースがNetAppストレージにあって保護されていない場合は、[Overall Status]列に「Not protected」と表示されます。
- データベースがNetAppストレージ システム上にあって保護されており、バックアップ処理が実行されていない場合は、[Overall Status]列に「Backup not run is displayed」と表示されます。それ以外の場合は、前回のバックアップ ステータスに基づいて、ステータスが「バックアップに失敗しました」または「バックアップに成功しました」に変わります。



SnapCenterの外部でデータベースの名前が変更された場合は、リソースを更新する必要があります。

手動でのプラグイン ホストへのリソースの追加

自動検出はWindowsホストではサポートされていません。Db2インスタンスとデータベース リソースは手動で追加する必要があります。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の設定などのタスクを完了しておく必要があります。

タスク概要

手動検出は、次の構成ではサポートされていません。

- RDMおよびVMDKレイアウト

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、ドロップダウン リストから [SnapCenter Plug-in for IBM Db2] を選択します。
2. [リソース] ページで、[IBM DB2 リソースの追加] をクリックします。
3. [Provide Resource Details]ページで、次の操作を実行します。

フィールド	操作
Name	データベース名を指定します。
Host Name	ホスト名を入力します。
タイプ	データベースまたはインスタンスを選択します。
Instance	データベースの親であるインスタンスの名前を指定します。
Credentials	クレデンシャルを選択するか、クレデンシャルの情報を追加します。 これはオプションです。

4. [ストレージ フットプリントの提供] ページで、ストレージ タイプを選択し、1 つ以上のボリューム、LUN、および qtree を選択して、[保存] をクリックします。

オプション：をクリックすることもできます  アイコンをクリックして、他のストレージ システムからボリューム、LUN、qtree を追加します。

5. オプション: リソース設定ページで、Windowsホスト上のリソースについては、IBM Db2プラグインのカスタムキーと値のペアを入力します。
6. 概要を確認し、[完了] をクリックします。

データベースは、ホスト名、関連するリソース グループとポリシー、全体的なステータスなどの情報とともに表示されます。

リソースへのアクセスをユーザに許可する場合は、ユーザにリソースを割り当てる必要があります。これにより、ユーザは、自身に割り当てられたアセットに対して、権限のある処理を実行できるようになります。

"ユーザまたはグループの追加と、ロールとアセットの割り当て"

データベースの追加が完了したら、IBM Db2データベースの詳細を変更できます。

IBM Db2のバックアップ ポリシーの作成

SnapCenterを使用してIBM Db2のリソースをバックアップする前に、バックアップ対象のリソースまたはリソース グループのバックアップ ポリシーを作成する必要があります。バックアップ ポリシーとは、バックアップをどのように管理し、スケジューリングし、保持するかを定める一連のルールです。

開始する前に

- バックアップ戦略を定義しておく必要があります。

詳細については、IBM Db2データベースのデータ保護戦略の定義に関する情報を参照してください。

- SnapCenterのインストール、ホストの追加、ストレージ システム接続の作成、リソースの追加などのタスクを実行して、データ保護の準備をしておく必要があります。
- ユーザがSnapshotをミラーまたはバックアップにレプリケートする場合は、ソース ボリュームとデスティネーション ボリューム両方のSVMをSnapCenter管理者がユーザに割り当てる必要があります。

ポリシーで、レプリケーション、スクリプト、アプリケーション設定を指定することもできます。それらのオプションを指定しておくことで、別のリソース グループにポリシーを再利用して時間を節約することができます。

タスク概要

- SnapLock
 - [Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで指定した保持日数以下にする必要があります。
 - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、ポリシーで指定した数よりも多くのSnapshotが保持される可能性があります。
 - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[ポリシー]をクリックします。
3. *新規*をクリックします。
4. 「名前」 ページで、ポリシー名と詳細を入力します。
5. [Policy type]ページで、次の手順を実行します。
 - a. ストレージ タイプを選択します。
 - b. カスタム バックアップ設定 セクションで、キーと値の形式でプラグインに渡す必要がある特定のバックアップ設定を指定します。

プラグインに渡すキーと値のペアを複数指定することができます。

6. スナップショットとレプリケーション ページで、次のアクションを実行します。

- a. オンデマンド、時間別、日次、週次、または*月次*を選択して、スケジュールの頻度を指定します。



リソース グループを作成する際に、バックアップ処理のスケジュール（開始日、終了日、頻度）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソース グループを作成できますが、各ポリシーに異なるバックアップ スケジュールを割り当てることもできます。



午前 2 時にスケジュールを設定した場合、夏時間 (DST) 中はスケジュールは実行されません。

- a. スナップショット設定セクションで、次のアクションを実行します。

状況	操作
特定の数のSnapshotを保持	*保持するコピー*を選択し、保持するスナップショットの数を指定します。 Snapshotの数が指定した数を超えると、古いものから順にSnapshotが削除されます。
Snapshotを特定の日数だけ保持	*コピーの保持期間*を選択し、スナップショットを削除する前に保持する日数を指定します。
スナップショットコピーのロック期間	スナップショット コピーのロック期間 を選択し、日、月、または年を指定します。 SnapLock保持期間は100年未満にする必要があります。



SnapshotコピーベースのバックアップでSnapVaultレプリケーションを有効にする場合は、保持数を2以上に設定する必要があります。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。

- b. ポリシーラベルを指定します。

リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしなくても実行できます。

7. [セカンダリ レプリケーション オプションの選択] セクションで、次のセカンダリ レプリケーション オプションの 1 つまたは両方を選択します。

フィールド	操作
Update SnapMirror after creating a local Snapshot copy	別のボリュームにバックアップ セットのミラー コピーを作成する場合（SnapMirrorレプリケーション）は、このフィールドを選択します。 このオプションは、SnapMirrorアクティブ同期に対して有効にする必要があります。
Update SnapVault after creating a local Snapshot copy	ディスクツーディスクのバックアップ レプリケーション（SnapVaultバックアップ）を実行する場合は、このオプションを選択します。
Error retry count	処理が停止されるまでに試行できるレプリケーションの最大回数を入力します。



セカンダリ ストレージでSnapshotの上限に達しないように、ONTAPでセカンダリ ストレージのSnapMirror保持ポリシーを設定する必要があります。

8. 概要を確認し、[完了] をクリックします。

リソース グループの作成とポリシーの適用

リソース グループはコンテナであり、バックアップして保護するリソースをここに追加する必要があります。リソース グループを使用することで、特定のアプリケーションに関連するすべてのデータを同時にバックアップできます。リソース グループはいずれのデータ保護ジョブにも必要になります。リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義することも必要です。

タスク概要

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。

フィールド	操作
Name	リソース グループの名前を入力します。 リソース グループ名は250文字以内で指定する必要があります。

フィールド	操作
Tags	リソース グループを検索しやすくするために、ラベルを入力します。 たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。
Use custom name format for snapshot copy	Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。 たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが附加されます。

4. [リソース] ページで、[ホスト] ドロップダウン リストからホスト名を選択し、[リソース タイプ] ドロップダウン リストからリソース タイプを選択します。

画面の情報がフィルタリングされます。

5. *利用可能なリソース*セクションからリソースを選択し、右矢印をクリックして*選択したリソース*セクションに移動します。
6. [Application Settings] ページで、次の操作を実行します。

- a. 追加のバックアップ オプションを設定するには、[バックアップ] 矢印をクリックします。

整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for Consistency Group snapshot operation to complete	スナップショット操作が完了するまでの待機時間を指定するには、「緊急」、「中」、または「緩和」を選択します。 [Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

+

- *スクリプト*矢印をクリックし、静止、スナップショット、および静止解除操作の事前および事後コマンドを入力します。障害の発生時に終了前に実行するプリコマンドも入力できます。
- *カスタム構成*矢印をクリックし、このリソースを使用するすべてのデータ保護操作に必要なカスタムのキーと値のペアを入力します。

パラメータ	設定	説明
ARCHIVE_LOG_ENABLE	(Y / N)	アーカイブ ログ管理を有効にし、アーカイブ ログを削除します。
ARCHIVE_LOG_RETENTION	number_of_days	アーカイブ ログを保持する日数を指定します。 この設定は、NTAP_SNAPSHOT_RETENTIONS 以上である必要があります。
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブ ログが含まれるディレクトリへのパスを指定します。
ARCHIVE_LOG_EXT	file_extension	アーカイブ ログ ファイルの拡張子の長さを指定します。 たとえば、アーカイブ ログが log_backup_0_0_0_0.161518551942 9 で、file_extension 値が 5 の場合、ログの拡張子は 5 桁、つまり 16151 になります。

パラメータ	設定	説明
ARCHIVE_LOG_RECURSIVE_SE ARCH	(Y / N)	サブディレクトリ内のアーカイブ ログの管理を有効にします。 アーカイブ ログがサブディレクトリの下にある場合は、このパラメータを使用する必要があります。



カスタムのキーと値のペアは、IBM Db2 Linuxプラグイン システムではサポートされますが、一元化されたWindowsプラグインとして登録されたIBM Db2データベースではサポートされません。

- c. スナップショット コピー ツール の矢印をクリックして、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する（このオプションはLinuxリソースには適用されません）	ファイル システムの一貫性を備えたSnapCenter * を選択します。
SnapCenterでストレージ レベルのSnapshotを作成する	ファイル システムの整合性のないSnapCenter * を選択します。
Snapshotを作成するためにホストで実行するコマンドを入力する	*その他*を選択し、スナップショットを作成するためにホスト上で実行するコマンドを入力します。

7. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます 。

ポリシーが[Configure schedules for selected policies]セクションのリストに表示されます。

- b. スケジュールの設定列で*をクリックします。 * 設定するポリシーの。
- c. ポリシー *policy_name* のスケジュールの追加ダイアログ ボックスでスケジュールを構成し、[OK] をクリックします。

*policy_name*は、選択したポリシーの名前です。

構成されたスケジュールは、「適用されたスケジュール」列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複してい

る場合、サポートされません。

8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP サーバーは、設定 > グローバル設定 で設定する必要があります。

9. 概要を確認し、[完了] をクリックします。

リソース グループを作成し、**ASA r2** システム上の **IBM Db2** リソースの二次保護を有効にします。

ASA r2 システム上にあるリソースを追加するには、リソース グループを作成する必要があります。リソース グループの作成時にセカンダリ保護をプロビジョニングすることもできます。

開始する前に

- ONTAP 9.x リソースとASA r2 リソースの両方を同じリソース グループに追加していないことを確認する必要があります。
- ONTAP 9.x リソースとASA r2 リソースの両方を含むデータベースが存在しないことを確認する必要があります。

タスク概要

- 二次保護は、ログインしたユーザーに **SecondaryProtection** 機能が有効になっているロールが割り当てられている場合にのみ使用できます。
- セカンダリ保護を有効にすると、プライマリおよびセカンダリ整合性グループの作成中にリソース グループはメンテナンス モードになります。プライマリおよびセカンダリのコンシステンシー グループが作成されると、リソース グループのメンテナンス モードが解除されます。
- SnapCenter はクローン リソースの二次保護をサポートしていません。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。
 - a. [Name] フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag] フィールドに1つ以上のラベルを入力します。

たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

- c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

たとえば、`customtext_resource group_policy_hostname`や`resource group_hostname`などの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- d. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。



必要に応じて、プレフィックスを含め、アプリケーションで設定されたのと同まったく同じ宛先を使用する必要があります。

4. [リソース] ページで、[ホスト] ドロップダウン リストからデータベース ホスト名を選択します。



[Available Resources]セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources]のリストには表示されません。

5. [使用可能なリソース] セクションからASA r2 リソースを選択し、[選択したリソース] セクションに移動します。
6. アプリケーション設定ページで、バックアップ オプションを選択します。
7. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックし  てポリシーを作成することもできます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。
- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 選択したポリシーに対して二次保護が有効になっている場合は、「二次保護」ページが表示されるので、次の手順を実行する必要があります。
- a. レプリケーション ポリシーのタイプを選択します。



同期レプリケーション ポリシーはサポートされていません。

- b. 使用する整合性グループのサフィックスを指定します。
- c. [宛先クラスタ] および [宛先 SVM] ドロップダウンから、使用するピア クラスタと SVM を選択します。



クラスターと SVM のピアリングはSnapCenterではサポートされていません。クラスターと SVM のピアリングを実行するには、System Manager またはONTAP CLI を使用する必要があります。



リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは [セカンダリ保護リソース] セクションに表示されます。

1. [Verification] ページで、次の手順を実行します。

- a. ロケータのロード をクリックして、 SnapMirrorまたはSnapVaultボリュームをロードし、セカンダリストレージで検証を実行します。
- b. クリック  ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で をクリックします。
- c. [Add Verification Schedules policy_name] ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

- d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証] を選択します。
- e. [OK] をクリックします。

設定した検証スケジュールが、[Applied Schedules] 列にリストされます。

2. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

3. 概要を確認し、[完了] をクリックします。

IBM Db2用のPowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成

PowerShellコマンドレットを使用してIBM Db2データベースのバックアップ、リストア、クローニングを行う前に、Storage Virtual Machine (SVM) 接続とクレデンシャルを作成する必要があります。

開始する前に

- PowerShellコマンドレットを実行できるようにPowerShell環境を準備しておく必要があります。
- ストレージ接続を作成するには、Infrastructure Adminロールの権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

ストレージ システム接続の追加中は、ホスト プラグインのインストールが進行中であってはなりません。ホスト キャッシュが更新されず、SnapCenter GUI にデータベースのステータスが「バックアップに使用できません」または「NetAppストレージ上にありません」と表示される可能性があるためです。

- ストレージ システムの名前は一意である必要があります。

SnapCenterでは、別々のクラスタに属している場合でも、複数のストレージ システムに同じ名前を付けることはサポートされません。SnapCenterでサポートする各ストレージ システムには、一意な名前とデータLIFの一意なIPアドレスが必要です。

手順

1. **SnapCenterPS** をクリックして PowerShell Core を起動します。
2. Add-SmStorageConnectionコマンドレットを使用して、ストレージ システムへの新しい接続を作成します。

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

3. Add-SmCredentialコマンドレットを使用して、新しいクレデンシャルを作成します。

この例は、Windowsクレデンシャルを使用してFinanceAdminという名前の新しいクレデンシャルを作成する方法を示しています。

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

4. SnapCenter ServerにIBM Db2通信ホストを追加します。

Linux :

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

Windows :

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

5. パッケージとSnapCenter Plug-in for IBM Db2をホストにインストールします。

Linux :

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

Windows :

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

6. SQLLIBのパスを設定します。

Windows の場合、Db2 プラグインは SQLLIB フォルダーのデフォルト パス「C:\Program Files\IBM\SQLLIB\BIN」を使用します。

デフォルト パスを上書きする場合は、次のコマンドを使用します。

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

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

Db2 データベースをバックアップする

データベースをバックアップするときは、SnapCenter Serverとの接続を確立してから、リソースの追加、ポリシーの追加、バックアップ リソース グループの作成を行って、バックアップを実行します。

開始する前に

- バックアップ ポリシーを作成しておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。
- Snapshotコピーベースのバックアップ処理の場合は、すべてのテナント データベースが有効でアクティブであることを確認してください。
- 休止、Snapshot、および休止解除の処理を実行するプリコマンドとポストコマンドの場合は、プラグインホストで次のパスから使用できるコマンド リストにコマンドがあるかどうかを確認する必要があります。
 - Windows ホスト上のデフォルトの場所: C:\Program Files\NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config

◦ Linux ホスト上のデフォルトの場所: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. リソース ページで、リソース タイプに基づいて 表示 ドロップダウン リストからリソースをフィルターします。

選択  をクリックし、ホスト名とリソース タイプを選択してリソースをフィルターします。次に選択できます  フィルター パネルを閉じます。

3. バックアップするリソースを選択します。
4. [リソース] ページで、[スナップショット コピーにカスタム名形式を使用する] を選択し、スナップショット名に使用するカスタム名形式を入力します。

たとえば、`customtext_policy_hostname` または `resource_hostname` です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

5. [Application Settings] ページで、次の操作を実行します。

- 追加のバックアップ オプションを設定するには、[バックアップ] 矢印を選択します。

必要に応じて、整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for "Consistency Group Snapshot" operation to complete	スナップショット操作が完了するまでの待機時間を指定するには、「緊急」、または「中」、または「緩和」を選択します。[Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

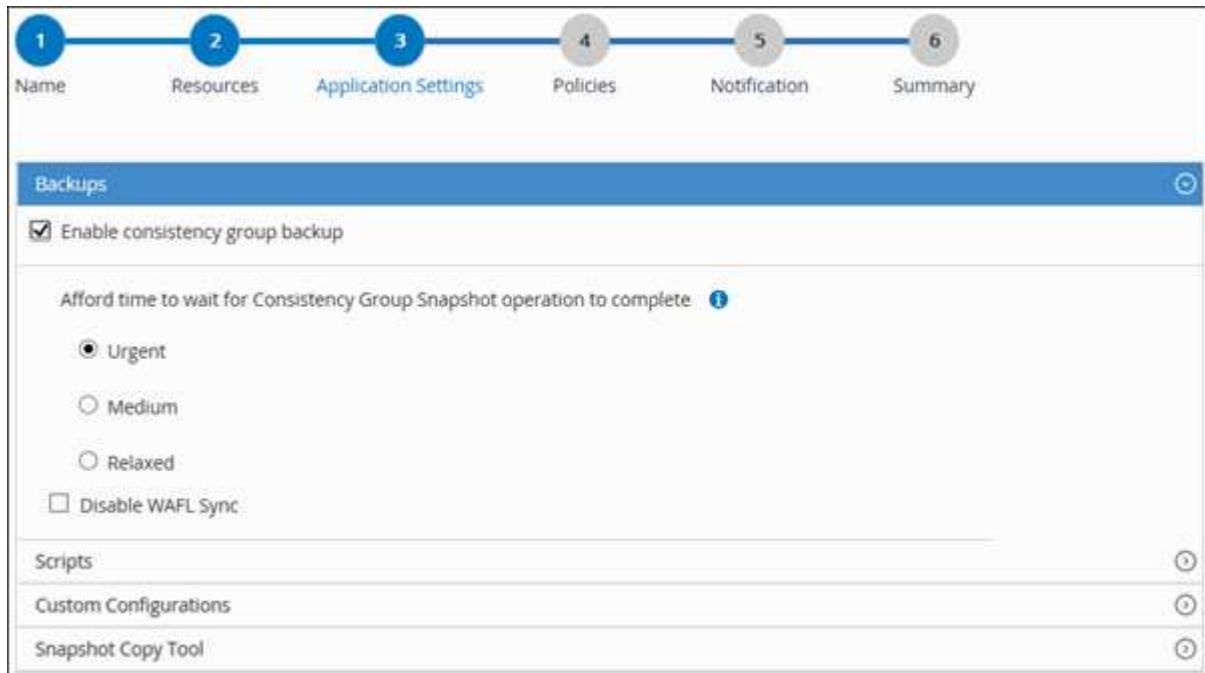
- *スクリプト*矢印を選択して、静止、スナップショット、および静止解除操作の事前および事後コマンドを実行します。

バックアップ処理を終了する前のプリコマンドも実行できます。プリスクリプトとポストスクリプトはSnapCenter Serverで実行されます。

- カスタム構成矢印を選択し、このリソースを使用するすべてのジョブに必要なカスタム値のペアを入力します。
- スナップショット コピー ツール 矢印を選択して、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでストレージ レベルのSnapshotを作成する	• ファイル システムの整合性のないSnapCenter * を選択します。

あなたが望むなら...	操作
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する	ファイル システムの一貫性を備えたSnapCenter * を選択します。
Snapshotを作成するためのコマンドを入力する	*その他*を選択し、スナップショットを作成するコマンドを入力します。



6. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます 。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b.  を選択 スケジュールを構成するポリシーの [スケジュールの構成] 列で、
- c. ポリシー *policy_name* のスケジュールの追加 ダイアログ ボックスでスケジュールを構成し、[OK] を選択します。

policy_name は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

7. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。

す。SMTP は、設定 > グローバル設定 でも設定する必要があります。

8. 概要を確認し、[完了] を選択します。

リソースのトポロジ ページが表示されます。

9. *今すぐバックアップ*を選択します。

10. [Backup]ページで次の手順を実行します。

- a. リソースに複数のポリシーを適用した場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*を選択します。

11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

- MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

詳細については、以下を参照してください。 ["MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"](#)

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmResourcesコマンドレットを使用して、手動リソースを追加します。

次の例では、IBM Db2インスタンスを追加する方法を示しています。

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

Db2データベースの場合：

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

3. Add-SmPolicyコマンドレットを使用して、バックアップ ポリシーを作成します。
4. リソースを保護するか、Add-SmResourceGroupコマンドレットを使用してSnapCenterに新しいリソース グループを追加します。
5. New-SmBackupコマンドレットを使用して、新しいバックアップ ジョブを開始します。

この例は、リソース グループをバックアップする方法を示しています。

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

次の例では、Db2インスタンスをバックアップしています。

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

次の例では、Db2データベースをバックアップしています。

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

6. Get-smJobSummaryReportコマンドレットを使用して、ジョブのステータス（実行中、完了、失敗）を確認します。

```
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. Get-SmBackupReport コマンドレットを使用して、リストアやクローニングの処理を実行するバックアップIDとバックアップ名など、バックアップジョブの詳細を監視します。

```

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

```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

リソース グループのバックアップ

リソース グループは、ホスト上のリソースの集まりです。リソース グループのバックアップ処理は、リソース グループに定義されているすべてのリソースを対象に実行されます。

開始する前に

- ポリシーを適用したリソース グループを作成しておく必要があります。

- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。

タスク概要

リソース グループは、[Resources]ページからオンデマンドでバックアップできます。リソース グループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが行われます。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。

リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、 をクリックして、タグを選択します。次に選択できます  フィルター パネルを閉じます。

3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] を選択します。
4. [Backup]ページで次の手順を実行します。
 - a. リソース グループに複数のポリシーを関連付けた場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*を選択します。
5. モニター > ジョブ を選択して、操作の進行状況を監視します。

IBM Db2バックアップ処理の監視

SnapCenterの[Jobs]ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*ジョブ*をクリックします。
3. [Jobs]ページで、次の手順を実行します。
 - a. をクリックして、 リストの内容をバックアップ処理だけに絞り込みます。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*バックアップ*を選択します。
 - d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. バックアップ ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスは  ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[Activity]ペインでのIBM Db2データベースに対するデータ保護処理の監視

[Activity]ペインには、最後に実行された5つの処理が表示されます。また[Activity]ペインには、処理が開始された日次と処理のステータスが表示されます。

[Activity]ペインには、バックアップ、リストア、クローニング、スケジュールされたバックアップの各処理に関する情報が表示されます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. クリック  アクティビティ ペインで、最新の 5 つの操作を表示します。

いずれかの操作をクリックすると、*ジョブの詳細*ページに操作の詳細が表示されます。

IBM Db2のバックアップ処理のキャンセル

キューに登録されているバックアップ処理はキャンセルできます。

必要なもの

- 処理をキャンセルするには、SnapCenter管理者かジョブ所有者としてログインする必要があります。
- バックアップ操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のバックアップ処理はキャンセルできません。
- バックアップ処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。

- キャンセルできない操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたバックアップ操作をキャンセルできます。

手順

1. 次のいずれかを実行します。

方法	アクション
[Monitor]ページ	a. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 b. 操作を選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	a. バックアップ操作を開始したら、*をクリックします。 * アクティビティ ペインで、最新の 5 つの操作を表示します。 b. 処理を選択します。 c. ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

処理がキャンセルされ、リソースは処理前の状態に戻ります。

[Topology]ページでのIBM Db2のバックアップとクローンの表示

リソースのバックアップまたはクローニングを準備する際に、プライマリ ストレージとセカンダリ ストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。

タスク概要

プライマリ ストレージまたはセカンダリ ストレージ（ミラー コピーまたはバックアップ コピー）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

- 
 プライマリ ストレージで使用可能なバックアップとクローンの数を表示します。
- 
 SnapMirrorテクノロジーを使用してセカンダリ ストレージにミラーリングされているバックアップとクローンの数を表示します。
- 
 SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップとクローンの数を表示します。



表示されるバックアップの数には、セカンダリ ストレージから削除されたバックアップも含まれます。たとえば、バックアップを4個保持するポリシーを使用してバックアップを6個作成した場合、バックアップの数は6個と表示されます。



mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジ ビューに表示されますが、トポロジ ビューのミラー バックアップの数にはバージョンに依存しないバックアップは含まれません。

[Topology]ページでは、選択したリソースまたはリソース グループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を参照し、対象を選択してデータ保護処理を実行できます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストからリソースまたはリソース グループを選択します。
3. リソースの詳細ビューまたはリソース グループの詳細ビューで、リソースを選択します。

リソースが保護されている場合は、選択したリソースのトポロジ ページが表示されます。

4. *概要カード*を確認して、プライマリ ストレージとセカンダリ ストレージで使用可能なバックアップとクローンの数の概要を確認します。

概要カード セクションには、スナップショット コピー ベースのバックアップとクローンの合計数が表示されます。

更新 ボタンをクリックすると、ストレージのクエリが開始され、正確な数が表示されます。

SnapLock対応バックアップが取得された場合、[更新] ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでも、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

アプリケーション リソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限はONTAPから取得されます。

オンデマンド バックアップ後、[更新] ボタンをクリックすると、バックアップまたはクローンの詳細が更新されます。

5. 「コピーの管理」ビューで、プライマリ ストレージまたはセカンダリ ストレージから バックアップ または クローンをクリックして、バックアップまたはクローンの詳細を表示します。

バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、削除の各処理を実行します。



セカンダリ ストレージ上のバックアップは、名前変更または削除できません。

7. クローンを削除する場合は、表でクローンを選択し、 をクリックします。

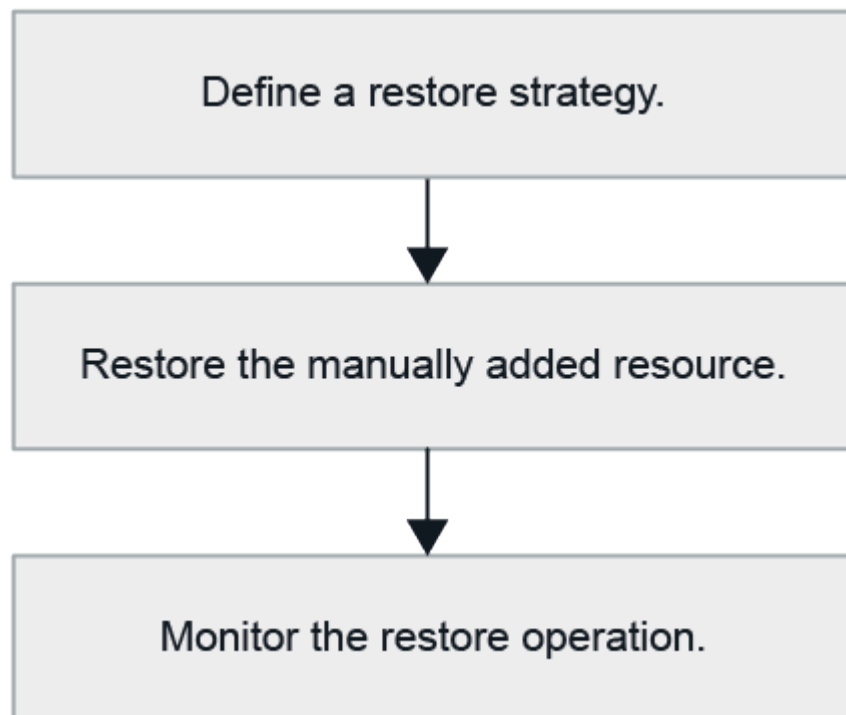
8. クローンを分割する場合は、テーブルからクローンを選択し、。

IBM Db2のリストア

リストアのワークフロー

リストアとリカバリのワークフローには、計画、リストア処理の実行、および処理の監視が含まれます。

次のワークフローは、リストア処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

手動で追加されたリソース バックアップのリストア

SnapCenterを使用して1つまたは複数のバックアップからデータをリストアおよびリカバリすることができます。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- リストアするリソースまたはリソース グループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- リストア前、リストア後、マウント、アンマウントの各コマンドを実行する場合は、プラグイン ホストで

次のパスから使用可能なコマンド リストにコマンドが存在するかどうかを確認する必要があります。

- Windows ホスト上のデフォルトの場所: `C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux ホスト上のデフォルトの場所: `/opt/ NetApp/ snapcenter/ scc/ etc/ allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホスト、関連するリソース グループとポリシー、およびステータスとともに表示されます。



リストアの実行時は、バックアップがリストア グループに対するものであっても、リストア対象のリソースを個別に選択する必要があります。

リソースが保護されていない場合は、「全体ステータス」列に「保護されていません」と表示されます。この状態になるのは、リソースが保護されていない場合とリソースが別のユーザによってバックアップされている場合です。

3. リソースを選択するか、リソース グループを選択してそのグループ内のリソースを選択します。

リソースのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージ システムから [バックアップ] を選択します。
5. プライマリバックアップテーブルで、復元するバックアップを選択し、*をクリックします。  *

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scspr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. 復元範囲ページで、*完全なリソース*を選択します。
 - a. *完全なリソース*を選択すると、IBM Db2 データベースのすべての構成済みデータ ボリュームが復元されます。

リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeのリストア用のSnapshotが選択されたあとに作成されたSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。

複数のLUNを選択できます。



すべて を選択すると、ボリューム、qtree、または LUN 上のすべてのファイルが復元されます。

7. [Pre ops] ページで、リストア ジョブの実行前に実行するリストア前の処理とアンマウントのコマン

ドを入力します。

8. [Post ops]ページで、リストア ジョブの実行後に実行するマウントとリストア後の処理のコマンドを入力します。
9. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP は、[設定] > [グローバル設定] ページでも設定する必要があります。

10. 概要を確認し、[完了] をクリックします。
11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

終了後の操作

ロールフォワード ステータスが「DB pending」の場合にのみリカバリが可能です。このステータスは、アーカイブ ログが有効なDb2データベースに適用されます。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよびGet-SmBackupReportコマンドレットを使用して、リストアするバックアップを特定します。

この例では、リストアできるバックアップが2つあります。

```
PS C:\> Get-SmBackup -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\Library
```

	BackupId	BackupName	BackupTime
BackupType			
	-----	-----	-----

	1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32
AM Full Backup			
	2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17
AM			

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId          : 113
SmJobId              : 2032
StartDateTime        : 2/2/2015 6:57:03 AM
EndDateTime          : 2/2/2015 6:57:11 AM
Duration             : 00:00:07.3060000
CreatedDateTime       : 2/2/2015 6:57:23 AM
Status               : Completed
ProtectionGroupName  : Clone
SmProtectionGroupId   : 34
PolicyName           : Vault
SmPolicyId           : 18
BackupName           : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus    : NotVerified

SmBackupId          : 114
SmJobId              : 2183
StartDateTime        : 2/2/2015 1:02:41 PM
EndDateTime          : 2/2/2015 1:02:38 PM
Duration             : -00:00:03.2300000
CreatedDateTime       : 2/2/2015 1:02:53 PM
Status               : Completed
ProtectionGroupName  : Clone
SmProtectionGroupId   : 34
PolicyName           : Vault
SmPolicyId           : 18
BackupName           : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus    : NotVerified
```

3. Restore-SmBackup コマンドレットを使用して、バックアップからデータをリストアします。



AppObjectId は「Host\Plugin\UID」です。ここで、UID = <instance_name> は手動で検出された DB2 インスタンス リソース用であり、UID = <instance_name>\<database_name> は IBM Db2 データベース リソース用です。ResourceId は、Get-smResources コマンドレットで取得できます。

```
Get-smResources -HostName cn24.sccore.test.com -PluginCode DB2
```

この例は、プライマリ ストレージからデータベースをリストアする方法を示しています。

```
Restore-SmBackup -PluginCode DB2 -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 3
```

この例は、セカンダリ ストレージからデータベースをリストアする方法を示しています。

```
Restore-SmBackup -PluginCode 'DB2' -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false  
-Archive @( @{"Primary"="<Primary  
Vserver>:<PrimaryVolume>";"Secondary"="<Secondary  
Vserver>:<SecondaryVolume>"})
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

自動検出されたデータベース バックアップのリストアとリカバリ

SnapCenterを使用して1つまたは複数のバックアップからデータをリストアおよびリカバリすることができます。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- リストアするリソースまたはリソース グループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- リストア前、リストア後、マウント、アンマウントの各コマンドを実行する場合は、プラグイン ホストで次のパスから使用可能なコマンド リストにコマンドが存在するかどうかを確認する必要があります。
 - Windows ホスト上のデフォルトの場所: *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
 - Linux ホスト上のデフォルトの場所: */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*



コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- 自動検出されたリソースについては、SFSRでリストアがサポートされます。
- 自動リカバリはサポートされていません。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。

2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホスト、関連するリソース グループとポリシー、およびステータスとともに表示されます。



リストアの実行時は、バックアップがリストア グループに対するものであっても、リストア対象のリソースを個別に選択する必要があります。

リソースが保護されていない場合は、「全体ステータス」列に「保護されていません」と表示されます。この状態になるのは、リソースが保護されていない場合とリソースが別のユーザによってバックアップされている場合です。

3. リソースを選択するか、リソース グループを選択してそのグループ内のリソースを選択します。

リソースのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボールド化された) ストレージシステムから [バックアップ] を選択します。

5. プライマリバックアップテーブルで、復元するバックアップを選択し、*をクリックします。  *。

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scscr0191683001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. 「復元範囲」 ページで、「完全なリソース」を選択して、IBM Db2 データベースの構成済みデータ ボリュームを復元します。
7. [Pre ops] ページで、リストア ジョブの実行前に実行するリストア前の処理とアンマウントのコマンドを入力します。

自動検出されたリソースについては、アンマウント コマンドは必須ではありません。

8. [Post ops] ページで、リストア ジョブの実行後に実行するマウントとリストア後の処理のコマンドを入力します。

自動検出されたリソースについては、マウント コマンドは必須ではありません。

9. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP は、[設定] > [グローバル設定] ページでも設定する必要があります。

10. 概要を確認し、[完了] をクリックします。
11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

終了後の操作

ロールフォワード ステータスが「DB pending」の場合にのみリカバリが可能です。このステータスは、アーカイブ ログが有効なDb2データベースに適用されます。

IBM Db2リストア処理の監視

[Job]ページを使用して、SnapCenterの各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  でリストをフィルタリングし、リストア処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*復元*を選択します。
 - d. *ステータス*ドロップダウンリストから、復元ステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. 復元ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

IBM Db2リソースのバックアップのクローニング

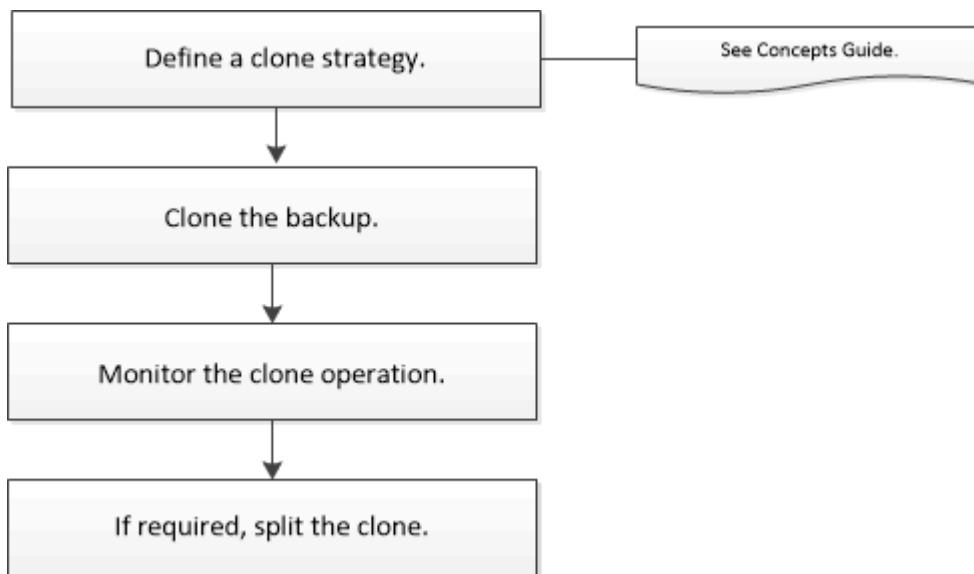
クローニングのワークフロー

クローニング ワークフローには、クローニング処理の実行と処理の監視が含まれます。

タスク概要

- ソースIBM Db2サーバでクローニング処理を実行できます。
- リソースのバックアップをクローニングする理由には次のものがあります。
 - アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のリソースの構造およびコンテンツを使用してテストするため
 - データの抽出と操作を行うツールで、データ ウェアハウスにデータを取り込むため
 - 誤って削除または変更されたデータをリカバリするため

次のワークフローは、クローニング処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

終了後の操作

自動検出されたDb2リソースをクローニングすると、クローン リソースは手動リソースとしてマークされます。クローンされた Db2 リソースを回復するには、「リソースの更新」をクリックします。クローンを削除すると、ストレージとホストもクリーンアップされます。

クローン処理後にリソースを更新せずにクローンを削除しようとする、ストレージとホストはクリーンアップされません。fstabでエントリを手動で削除する必要があります。

IBM Db2バックアップのクローニング

SnapCenterを使用してバックアップをクローニングすることができます。クローニングはプライマリとセカンダリのどちらのバックアップからも実行できます。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- ボリュームをホストするアグリゲートがStorage Virtual Machine (SVM) の割り当て済みアグリゲート リストに含まれていることを確認します。
- 代替ホスト上に Db2 のクローンを作成するときは、他のホスト上の元のマウント パスと同じクローン マウント パスの n-1 ディレクトリ構造を作成する必要があります。マウント パスには 755 実行権限が必要です。
- クローニング前またはクローニング後のコマンドについては、プラグイン ホストの次のパスで使用できるコマンド リストにコマンドが存在するかどうかを確認する必要があります。
 - Windows ホスト上のデフォルトの場所: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux ホスト上のデフォルトの場所: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- FlexCloneボリューム分割操作の詳細については、以下を参照してください。 <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["親ボリュームからのFlexCloneボリュームのスプリット"]。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホスト、関連するリソース グループとポリシー、ステータスなどの情報とともに表示されます。

3. リソースまたはリソース グループを選択します。

リソース グループを選択した場合はリソースを選択する必要があります。

リソースまたはリソース グループのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージ システムから [バックアップ] を選択します。
5. 表からデータバックアップを選択し、クリックします。 。
6. [Location] ページで、次の操作を実行します。

フィールド	操作
Clone server	クローンをどのホスト上に作成するかを選択します。
Target Clone Instance	既存のバックアップからクローニングするターゲットのDb2クローン インスタンスIDを入力します。 これは、ANFストレージ タイプのリソースにのみ該当します。
Target Clone Name	クローンの名前を入力します。 これは、Db2データベース リソースにのみ該当します。
NFS Export IP Address	クローン ボリュームをエクスポートするホスト名またはIPアドレスを入力します。 これは、NFSストレージ タイプのリソースにのみ該当します。
Capacity Pool Max. Throughput (MiB/s)	容量プールの最大スループットを入力します。

7. [Scripts] ページで、次の手順を実行します。



スクリプトはプラグイン ホストで実行されます。

- a. クローニング処理の前後に実行するプリコマンドやポストコマンドを入力します。
 - クローニング前のコマンド：同じ名前の既存のデータベースの削除
 - クローニング後のコマンド：データベースの検証やデータベースの起動
- b. ホストにファイルシステムをマウントするには、mountコマンドを入力します。

Linuxマシンのボリュームまたはqtreeに対するmountコマンド：

NFSの例: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。

9. 概要を確認し、[完了] をクリックします。
10. モニター > ジョブ をクリックして、操作の進行状況を監視します。

終了後の操作

自動検出されたDb2リソースをクローニングすると、クローン リソースは手動リソースとしてマークされます。クローンされた Db2 リソースを回復するには、「リソースの更新」をクリックします。クローンを削除すると、ストレージとホストもクリーンアップされます。

クローン処理後にリソースを更新せずにクローンを削除しようとする、ストレージとホストはクリーンアップされません。fstabでエントリを手動で削除する必要があります。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. クローニングできるバックアップの一覧を表示するには、Get-SmBackupコマンドレットかGet-SmResourceGroupコマンドレットを使用します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

この例では、指定したリソース グループとそのリソース、および関連ポリシーに関する情報を表示しています。

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
```

Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}


```

AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False

```

3. 既存のバックアップからのクローニング処理を開始するには、New-SmCloneコマンドレットを使用します。

この例では、指定したバックアップからすべてのログを含めてクローンを作成しています。

```

PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

この例では、指定したMicrosoft SQL Serverインスタンスのクローンを作成しています。

```

PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"

```

4. クローニング ジョブのステータスを表示するには、Get-SmCloneReportコマンドレットを使用します。

この例では、指定したジョブIDのクローン レポートを表示しています。

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

IBM Db2のクローニング処理の監視

SnapCenterのクローニング処理の進捗状況を、[Jobs]ページで監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター* ページで、*ジョブ* をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  でリストをフィルタリングし、クローニング処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ* ドロップダウンリストから*クローン*を選択します。
 - d. *ステータス* ドロップダウンリストからクローンのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. クローンジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. ジョブの詳細ページで、*ログの表示* をクリックします。

クローンのスプリット

SnapCenterを使用して、クローン リソースを親リソースからスプリットできます。スプリットされたクローンは親リソースから独立します。

タスク概要

- 中間クローンではクローン スプリット処理を実行できません。

たとえば、データベース バックアップからクローン1を作成したあとで、クローン1のバックアップを作成し、そのバックアップ（クローン2）をクローニングできます。クローン2を作成すると、クローン1は中間クローンになり、クローン1ではクローン スプリット処理を実行できなくなります。ただし、クローン2に対してはクローン スプリット処理を実行できます。

クローン2をスプリットすると、クローン1は中間クローンではなくなるため、クローン1に対してクローン スプリット処理を実行できるようになります。

- クローンをスプリットすると、そのクローンのバックアップ コピーとクローン ジョブが削除されます。
- FlexCloneボリューム分割操作の詳細については、以下を参照してください。 ["親ボリュームからのFlexCloneボリュームのスプリット"](#)。
- ストレージ システム上のボリュームまたはアグリゲートがオンラインであることを確認します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. *リソース* ページで、表示リストから適切なオプションを選択します。

オプション	説明
データベース アプリケーションの場合	表示リストから*データベース*を選択します。
ファイルシステムの場合	表示リストから*パス*を選択します。

3. リストから適切なリソースを選択します。

リソースのトポロジ ページが表示されます。

4. *コピーの管理*ビューから、クローンされたリソース（データベースやLUNなど）を選択し、*をクリックします。  *。
5. 分割するクローンの推定サイズとアグリゲート上で必要な空き容量を確認し、[開始] をクリックします。
6. モニター > ジョブ をクリックして、操作の進行状況を監視します。

SMCoreサービスが再起動されると、クローン スプリット処理は応答を停止します。Stop-SmJobコマンドレットを実行してクローン スプリット処理を停止してから、クローン スプリット処理を再試行してください。

クローンが分割されているかどうかを確認するためのポーリング時間を長くしたり短くしたりする場合は、*SMCoreServiceHost.exe.config* ファイルの *CloneSplitStatusCheckPollTime* パラメータの値を変更して、SMCore がクローン分割操作のステータスをポーリングする時間間隔を設定できます。値はミリ秒単位で、デフォルト値は5分です。

例えば：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

バックアップ、リストア、または別のクローン スプリットが実行中の場合、クローン スプリットの開始処理は失敗します。クローン スプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

["アグリゲートが存在しないためにSnapCenterのクローニングや検証が失敗する"](#)

SnapCenterアップグレード後のIBM Db2データベースのクローンの削除またはスプリット

SnapCenter 4.3にアップグレードすると、クローンは表示されなくなります。クローンを作成したリソースの[Topology]ページで、クローンの削除やスプリットを実行できます。

タスク概要

非表示のクローンのストレージ フットプリントを見つける場合は、次のコマンドを実行します。Get-SmClone -ListStorageFootprint

手順

1. remove-smbbackupコマンドレットを使用して、クローニングされたリソースのバックアップを削除します。
2. remove-smresourcegroupコマンドレットを使用して、クローニングされたリソースのリソース グループを削除します。
3. remove-smprotectresourceコマンドレットを使用して、クローニングされたリソースの保護を解除します。
4. [Resources]ページで親リソースを選択します。

リソースのトポロジ ページが表示されます。

5. [Manage Copies]ビューで、プライマリまたはセカンダリ（ミラー先またはレプリケート先）ストレージシステムからクローンを選択します。
6. クローンを選択し、クリックします  クローンを削除するには、または  クローンを分割します。
7. [OK]をクリックします。

PostgreSQLの保護

SnapCenter Plug-in for PostgreSQL

SnapCenter Plug-in for PostgreSQLの概要

SnapCenter Plug-in for PostgreSQL クラスタは、PostgreSQL クラスタに対してアプリケーション対応のデータ保護管理を可能にする、NetApp SnapCenter ソフトウェアのホスト側コンポーネントです。Plug-in for PostgreSQL クラスタは、SnapCenter 環境での PostgreSQL クラスタのバックアップ、リストア、およびクローニングを自動化します。

SnapCenter は、シングル クラスタとマルチ クラスタの PostgreSQL セットアップをサポートしています。Plug-in for PostgreSQL クラスタは、Windows と Linux のどちらの環境でも使用できます。Windows 環境では、PostgreSQL は手動リソースとしてサポートされます。

Plug-in for PostgreSQL クラスタがインストールされている場合は、SnapCenter と NetApp SnapMirror テクノロジを使用して、バックアップ セットのミラー コピーを別のボリュームに作成できます。また、このプラグインを NetApp SnapVault テクノロジとともに使用して、標準への準拠を目的としたディスクツーディスク バックアップ レプリケーションを実行することもできます。

SnapCenter Plug-in for PostgreSQL は、ONTAP および Azure NetApp Files ストレージ レイアウトで NFS と SAN をサポートします。

VMDK、vVol、RDM 仮想ストレージ レイアウトがサポートされています。

SnapCenter Plug-in for PostgreSQLの機能

Plug-in for PostgreSQL クラスタをインストールした環境では、SnapCenter を使用して PostgreSQL クラスタとそのリソースをバックアップ、リストア、クローニングできます。これらの処理をサポートするタスクも実行できます。

- クラスタを追加します。
- バックアップを作成します。
- バックアップからリストアします。
- バックアップをクローニングします。
- バックアップ処理のスケジュールを設定します。
- バックアップ、リストア、クローニングの各処理を監視します。
- バックアップ、リストア、クローニングの各処理のレポートを表示します。

SnapCenter Plug-in for PostgreSQLの特長

SnapCenter は、プラグイン アプリケーションと統合されるほか、ストレージ システム上で NetApp の数々のテクノロジーと統合されます。Plug-in for PostgreSQL クラスタの操作には、SnapCenter のグラフィカル ユーザ インターフェイスを使用します。

- 統合されたグラフィカルユーザーインターフェース

SnapCenterのインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。どのプラグインでも、SnapCenterのインターフェイスから、バックアップ、リストア、クローニングの各処理を一貫した方法で実行できるほか、ダッシュボード ビューで概要を把握したり、ロールベース アクセス制御 (RBAC) を設定したり、ジョブを監視したりすることができます。

- 自動化された中央管理

バックアップ処理のスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理を実行したりできます。SnapCenterからのEメール アラートの送信を設定して、環境をプロアクティブに監視することもできます。

- 無停止の**NetApp**スナップショット コピー テクノロジー

SnapCenterでは、Plug-in for PostgreSQLクラスタでNetApp Snapshotテクノロジーを使用してリソースがバックアップされます。

Plug-in for PostgreSQLを使用すると、次のメリットもあります。

- バックアップ、リストア、およびクローニングのワークフローがサポートされます。
- セキュリティがRBACでサポートされ、ロール委譲が一元化されます。

クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルのアクセス権を付与することもできます。

- NetApp FlexCloneテクノロジーを使用して、テストまたはデータ抽出に使用するリソースのコピー（スペース効率に優れたポイントインタイム コピー）を作成できます。

クローンを作成するストレージ システムにFlexCloneライセンスが必要です。

- バックアップの作成でONTAPの整合グループ（CG）のSnapshot機能がサポートされます。
- 複数のリソース ホストで同時に複数のバックアップを実行できます。

1回の処理で、1つのホストの複数のリソースが同じボリュームを共有する場合に複数のSnapshotが統合されます。

- 外部コマンドを使用してSnapshotを作成できます。
- XFSファイルシステム上のLinux LVMがサポートされます。

SnapCenter Plug-in for PostgreSQLでサポートされるストレージ タイプ

SnapCenterは、物理マシンと仮想マシン（VM）の両方でさまざまなストレージ タイプをサポートしています。SnapCenter Plug-in for PostgreSQLをインストールする前に、ストレージ タイプがサポートされているかどうかを確認する必要があります。

マシン	ストレージ タイプ
物理サーバ	• FC接続LUN • iSCSI接続LUN • NFS接続ボリューム
VMware ESXi	• FCまたはiSCSI HBAで接続されたRDM LUNホスト バス アダプタ (HBA) のスキャン は、SnapCenterがホストに存在するすべてのホスト バス アダプタをスキャンするため、完了までに時間がかかることがあります。 <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> にある LinuxConfig.pm ファイルを編集し て、SCSI_HOSTS_OPTIMIZED_RESCAN パラメータの値を 1 に設定し、HBA_DRIVER_NAMES にリストされているHBA のみを再スキャンすることができます。 • iSCSIイニシエータでゲスト システムに直接接続されたiSCSI LUN • NFSデータストア上のVMDK • VMFS上のVMDK • ゲスト システムに直接接続されたNFSボリューム • NFSとSANの両方に存在するvVolデータストア vVolデータストアは、ONTAP Tools for VMware vSphereでのみプロビジョニングできます。

PostgreSQLプラグインに必要な最小ONTAP権限

必要な最小ONTAP権限は、データ保護に使用するSnapCenterプラグインによって異なります。

- 全アクセス コマンド: ONTAP 9.12.1 以降に必要な最小限の権限
 - event generate-autosupport-log
 - job history show
 - job stop
 - lun
 - lun create
 - lun create

- lun create
- lun delete
- lun igroup add
- lun igroup create
- lun igroup delete
- lun igroup rename
- lun igroup rename
- lun igroup show
- lun mapping add-reporting-nodes
- lun mapping create
- lun mapping delete
- lun mapping remove-reporting-nodes
- lun mapping show
- lun modify
- lun move-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- lun resize
- lun serial
- lun show
- snapmirror policy add-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- snapmirror restore
- snapmirror show
- snapmirror show-history
- snapmirror update
- snapmirror update-ls-set
- snapmirror list-destinations
- version
- volume clone create
- volume clone show
- volume clone split start
- volume clone split stop
- volume create

- volume destroy
- volume file clone create
- volume file show-disk-usage
- volume offline
- volume online
- volume modify
- volume qtree create
- volume qtree delete
- volume qtree modify
- volume qtree show
- volume restrict
- volume show
- volume snapshot create
- volume snapshot delete
- volume snapshot modify
- volume snapshot modify-snaplock-expiry-time
- volume snapshot rename
- volume snapshot restore
- volume snapshot restore-file
- volume snapshot show
- volume unmount
- vservers cifs
- vservers cifs share create
- vservers cifs share delete
- vservers cifs shadowcopy show
- vservers cifs share show
- vservers cifs show
- vservers export-policy
- vservers export-policy create
- vservers export-policy delete
- vservers export-policy rule create
- vservers export-policy rule show
- vservers export-policy show
- vservers iscsi
- vservers iscsi connection show
- vservers show

- 読み取り専用コマンド: ONTAP 8.3.0以降に必要な最小限の権限

- ネットワークインターフェース
- network interface show
- SVM

PostgreSQLでのSnapMirrorレプリケーションとSnapVaultレプリケーションのためのストレージシステムの準備

SnapCenterプラグインと一緒にONTAP SnapMirrorテクノロジーを使用すると、バックアップセットのミラー コピーを別のボリュームに作成できます。また、ONTAP SnapVaultを使用すれば、標準への準拠やその他のガバナンスを目的としたディスクツェーディスクのバックアップ レプリケーションを実行できます。これらのタスクを実行する前に、ソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenterは、Snapshot処理の完了後に、SnapMirrorとSnapVaultに対する更新を実行します。SnapMirror更新とSnapVault更新は、SnapCenterジョブの一部として実行されるため、ONTAPスケジュールを別途作成しないでください。



NetApp SnapManager製品からSnapCenterに移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリ ストレージ（ソース ボリューム）上のデータがセカンダリ ストレージ（デスティネーション ボリューム）にレプリケートされます。この関係を初期化すると、ソース ボリュームで参照されるデータ ブロックがデスティネーション ボリュームに転送されます。



SnapCenter は、SnapMirrorとSnapVaultボリューム間のカスケード関係をサポートしていません（* プライマリ * > ミラー > ボールト）。ファンアウト関係を使用する必要があります。

SnapCenterは、バージョンに依存しないSnapMirror関係の管理をサポートしています。バージョンに依存しないSnapMirror関係とその設定方法の詳細については、["ONTAPのドキュメント"](#)。

PostgreSQLのバックアップ戦略

PostgreSQLのバックアップ戦略の定義

バックアップ ジョブを作成する前にバックアップ戦略を定義しておく、リソースの正常なリストアやクローニングに必要なバックアップを作成するのに役立ちます。バックアップ戦略の大部分は、サービス レベル アグリーメント（SLA）、目標復旧時間（RTO）、および目標復旧時点（RPO）によって決まります。

タスク概要

SLAとは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。RTOは、サービスの停止からビジネス プロセスの復旧までに必要となる時間です。RPOは、障害発生後に通常処理を再開するためにバックアップ ストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA、RTO、およびRPOは、データ保護戦略に関与します。

手順

1. リソースをバックアップするタイミングを決定します。
2. 必要なバックアップ ジョブの数を決定します。
3. バックアップの命名方法を決定します。
4. Snapshotコピーベースのポリシーを作成してアプリケーションと整合性のあるクラスタのSnapshotをバックアップするかどうかを決定します。
5. レプリケーションのためにNetApp SnapMirrorテクノロジーを使用するか、または長期保持のためにNetApp SnapVaultテクノロジーを使用するかを決定します。
6. ソース ストレージ システムおよびSnapMirrorデスティネーションでのSnapshotの保持期間を確認します。
7. バックアップ処理の前後にコマンドを実行するかどうかを決定し、実行する場合はプリスクリプトまたはポストスクリプトを用意します。

Linuxホスト上のリソースの自動検出

リソースとは、SnapCenterで管理するLinuxホスト上のPostgreSQLクラスタとインスタンスです。SnapCenter Plug-in for PostgreSQLプラグインをインストールすると、そのLinuxホスト上のすべてのインスタンスのPostgreSQLクラスタが自動的に検出されて[Resources]ページに表示されます。

サポートされるバックアップのタイプ

バックアップ タイプでは、作成するバックアップのタイプを指定します。SnapCenterでは、PostgreSQLクラスタに対してSnapshotコピーベースのバックアップ タイプがサポートされます。

Snapshotコピーベースのバックアップ

Snapshotコピーベースのバックアップでは、NetApp Snapshotテクノロジーを利用して、PostgreSQLクラスタが格納されたボリュームのオンラインの読み取り専用のコピーが作成されます。

SnapCenter Plug-in for PostgreSQLでの整合グループSnapshotの使用方法

プラグインを使用して、リソース グループの整合グループSnapshotを作成することができます。整合グループとはボリュームのコンテナであり、複数のボリュームを格納して1つのエンティティとして管理できます。整合グループには複数のボリュームの同時に作成されたSnapshotが格納されるため、一連のボリュームのコピーの整合性が確保されます。

ストレージ コントローラが整合性を確保しながらSnapshotをグループ化するのを待機する時間も指定できます。利用可能な待機時間のオプションは、「緊急」、「中」、「緩和」です。また、整合グループSnapshotの処理でWrite Anywhere File Layout (WAFL) の同期を有効にするか無効にするかも選択できます。WAFLの同期を有効にすると、整合グループSnapshotのパフォーマンスが向上します。

SnapCenterによる不要なデータ バックアップの削除の管理

SnapCenterは、ストレージ システム レベルおよびファイルシステム レベルで不要なデ

ータバックアップの削除を管理します。

保持設定に基づいて、プライマリストレージまたはセカンダリストレージのSnapshotが削除され、PostgreSQLのカatalog内の対応するエントリも削除されます。

PostgreSQLのバックアップスケジュールを決定する際の考慮事項

バックアップのスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率です。使用頻度の高いリソースは1時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは1日に1回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービスレベルアグリーメント（SLA）、目標復旧時点（RPO）などがあります。

バックアップスケジュールには、次の2つの要素があります。

- バックアップ頻度（バックアップを実行する間隔）

バックアップ頻度は、ポリシー設定の一部であり、一部のプラグインではスケジュールタイプとも呼ばれます。たとえば、毎時、毎日、毎週、または毎月としてバックアップ頻度を設定できます。

- バックアップスケジュール（バックアップが実行される日時）

バックアップスケジュールは、リソースまたはリソースグループの設定の一部です。たとえば、週次バックアップのポリシーが設定されているリソースグループがある場合、毎週木曜日の午後10時にバックアップするようにスケジュールを設定できます。

PostgreSQLに必要なバックアップジョブの数

必要なバックアップジョブの数を左右する要因としては、リソースのサイズ、使用中のボリュームの数、リソースの変更率、サービスレベルアグリーメント（SLA）などがあります。

Plug-in for PostgreSQL クラスタのバックアップの命名規則

Snapshotのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則ではSnapshot名にタイムスタンプが追加されるので、コピーが作成されたタイミングを特定できます。

Snapshotでは、次のデフォルトの命名規則が使用されます。

```
resourcegroupname_hostname_timestamp
```

バックアップリソースグループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- *dts1* はリソース グループ名です。
- *mach1x88* はホスト名です。
- *03-12-2015_23.17.26* は日付とタイムスタンプです。

または、[スナップショット コピーにカスタム名形式を使用する] を選択して、リソースまたはリソース グループを保護しながらスナップショット名の形式を指定することもできます。たとえば、*customtext_resourcegroup_policy_hostname*や*resourcegroup_hostname*などの形式です。デフォルトでは、Snapshot名にタイムスタンプのサフィックスが追加されます。

PostgreSQLのリストアとリカバリの戦略

PostgreSQLリソースのリストアとリカバリの戦略の定義

クラスタのリストアとリカバリを行う前に戦略を定義しておく、リストア処理とリカバリ処理を正常に実行できるようになります。



クラスタの手動リカバリのみがサポートされます。

手順

1. 手動で追加したPostgreSQLリソースでサポートされるリストア戦略を確認します。
2. 自動検出されたPostgreSQLクラスタでサポートされるリストア戦略を確認します。
3. 実行するリカバリ処理のタイプを決定します。

手動で追加したPostgreSQLリソースでサポートされるリストア戦略のタイプ

SnapCenterを使用してリストア処理を正常に実行するには、戦略を定義しておく必要があります。



手動で追加したPostgreSQLリソースはリカバリできません。

リソース全体のリストア

- リソースのすべてのボリューム、qtree、およびLUNをリストア



リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeのリストア用のSnapshotが選択されたあとに作成されたSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。

注意: PostgreSQL 用プラグインは、手動での復元を支援するために、`<OS_temp_folder>/postgresql_sc_recovery<Restore_JobId>/` フォルダーに `backup_label` と `tablespace_map` を作成します。

自動検出されたPostgreSQLでサポートされるリストア戦略のタイプ

SnapCenterを使用してリストア処理を正常に実行するには、戦略を定義しておく必要が

あります。

リソースの完全なリストアは、自動検出されたPostgreSQLクラスタに対してサポートされているリストア戦略です。この戦略では、リソースのすべてのボリューム、qtree、およびLUNがリストアされます。

自動検出された**PostgreSQL**のリストア処理のタイプ

SnapCenter Plug-in for PostgreSQLでは、自動検出されたPostgreSQLクラスタに対して、Single File SnapRestoreおよびConnect and Copyリストアタイプがサポートされます。

NFS環境でSingle File SnapRestoreを実行するシナリオは、次のとおりです。

- *完全なリソース*オプションのみを選択した場合
- 選択したバックアップがSnapMirrorまたはSnapVaultのセカンダリロケーションからのものであり、*完全なリソース*オプションが選択されている場合

SAN環境でSingle File SnapRestoreを実行するシナリオは、次のとおりです。

- *完全なリソース*オプションのみを選択した場合
- バックアップがSnapMirrorまたはSnapVaultのセカンダリロケーションから選択され、*完全なリソース*オプションが選択されている場合

PostgreSQLクラスタでサポートされるリカバリ処理のタイプ

SnapCenterでは、PostgreSQLクラスタに対してさまざまなタイプのリカバリ処理を実行できます。

- クラスタを最新の状態までリカバリする
- クラスタを特定の時点までリカバリする

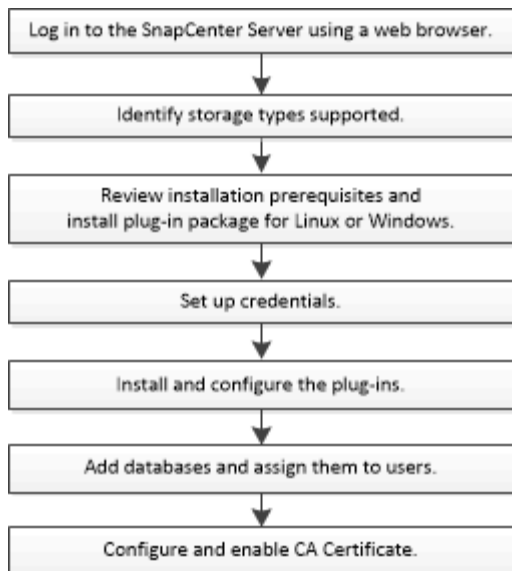
リカバリの日時を指定する必要があります。

SnapCenterでは、PostgreSQLクラスタに対して[No recovery]オプションも用意しています。

SnapCenter Plug-in for PostgreSQLのインストール準備

SnapCenter Plug-in for PostgreSQLのインストール ワークフロー

PostgreSQLクラスタを保護する場合は、SnapCenter Plug-in for PostgreSQLをインストールしてセットアップする必要があります。



ホストを追加して**SnapCenter Plug-in for PostgreSQL**をインストールするための前提条件

ホストを追加してプラグイン パッケージをインストールする前に、すべての要件を満たしておく必要があります。SnapCenter Plug-in for PostgreSQLは、WindowsとLinuxどちらの環境でも使用できます。

- Java 11をホストにインストールしておく必要があります。



IBM Java は Windows および Linux ホストではサポートされていません。

- Windows の場合、プラグイン クリエーター サービスは、“LocalSystem” Windows ユーザーを使用して実行する必要があります。これは、PostgreSQL 用プラグインがドメイン管理者としてインストールされている場合のデフォルトの動作です。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。WindowsホストにPostgreSQLプラグインをインストールすると、SnapCenter Plug-in for Microsoft Windowsもデフォルトで導入されます。
- SnapCenter Serverが、Plug-in for PostgreSQLホストの8145ポートまたはカスタム ポートにアクセスできる必要があります。

Windowsホスト

- ローカル管理者権限があり、リモート ホストに対してローカル ログインのアクセス許可があるドメイン ユーザが必要です。
- Plug-in for PostgreSQLをWindowsホストにインストールすると、SnapCenter Plug-in for Microsoft Windowsが自動的にインストールされます。
- rootユーザまたはroot以外のユーザに対してパスワード ベースのSSH接続を有効にしておく必要があります。
- Java 11をWindowsホストにインストールしておく必要があります。

["すべてのオペレーティングシステム用のJAVAをダウンロード"](#)

Linuxホスト

- rootユーザまたはroot以外のユーザに対してパスワード ベースのSSH接続を有効にしておく必要があります。
- Java 11をLinuxホストにインストールしておく必要があります。

"すべてのオペレーティングシステム用のJAVAをダウンロード"

"NetApp Interoperability Matrix Tool"

- LinuxホストでPostgreSQLクラスタを実行している場合は、Plug-in for PostgreSQLのインストール時にSnapCenter Plug-in for UNIXが自動的にインストールされます。
- プラグインのインストールには、デフォルトのシェルとして **bash** を使用する必要があります。

補助コマンド

SnapCenterプラグイン for PostgreSQL で補足コマンドを実行するには、そのコマンドを *allowed_commands.config* ファイルに含める必要があります。

- Windows ホスト上のデフォルトの場所: *C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Linux ホスト上のデフォルトの場所: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

プラグイン ホストで補足コマンドを許可するには、エディターで *allowed_commands.config* ファイルを開きます。各コマンドを別々の行に入力します。コマンドでは大文字と小文字は区別されません。完全修飾パス名を指定し、パス名にスペースが含まれている場合は引用符 (") で囲んでください。

例えば：

コマンド: mount コマンド: umount コマンド: "C:\Program Files\ NetApp\ SnapCreator commands\sdcli.exe" コマンド: myscript.bat

allowed_commands.config ファイルが存在しない場合、コマンドまたはスクリプトの実行はブロックされ、ワークフローは次のエラーで失敗します。

"[/mnt/mount -a] の実行は許可されていません。Authorize by adding the command in the file %s on the plugin host."

コマンドまたはスクリプトが *allowed_commands.config* に存在しない場合、コマンドまたはスクリプトの実行はブロックされ、ワークフローは次のエラーで失敗します。

"[/mnt/mount -a] の実行は許可されていません。Authorize by adding the command in the file %s on the plugin host."



すべてのコマンドを許可するには、ワイルドカード エントリ (*) を使用しないでください。

Linuxホストのroot以外のユーザへのsudo権限の設定

SnapCenter、非ルート ユーザーが Linux 用のSnapCenterプラグイン パッケージをインストールし、プラグイン プロセスを開始できます。プラグイン プロセスは有効なroot以外のユーザとして実行されます。いくつかのパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

必要なもの

- sudoバージョン1.8.7以降
- umask が 0027 の場合、java フォルダーとその中のすべてのファイルに 555 の権限があることを確認します。そうしないと、プラグインのインストールが失敗する可能性があります。
- root以外のユーザについては、root以外のユーザの名前とユーザのグループが同じであることを確認してください。
- `/etc/ssh/sshd_config` ファイルを編集して、メッセージ認証コード アルゴリズム (MAC hmac-sha2-256 および MAC hmac-sha2-512) を設定します。

この構成ファイルを更新したら、sshdサービスを再起動します。

例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

このタスクについて

次のパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

- `/home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall`
- `/custom_location/NetApp/snapcenter/spl/bin/spl`

手順

1. SnapCenter Plug-ins Package for LinuxをインストールするLinuxホストにログインします。
2. visudo Linuxユーティリティを使用して、`/etc/sudoers`ファイルに次の行を追加します。

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Precchecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```

`LINUX_USER` は、作成した非 root ユーザーの名前です。

`checksum_value` は、次の場所にある `sc_unix_plugins_checksum.txt` ファイルから取得できます。

- `_C:\ProgramData\NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _` (SnapCenter Server が Windows ホストにインストールされている場合)。
- `/_opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _` SnapCenter Server が Linux ホストにインストールされている場合。



この例は、独自のデータを作成する際の参照としてのみ使用してください。

SnapCenter Plug-ins Package for Windowsをインストールするホストの要件

SnapCenter Plug-ins Package for Windowsをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	Microsoft Windows サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB

項目	要件
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	5 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell Core 7.4.2 サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。

SnapCenter Plug-ins Package for Linuxをインストールするホストの要件

SnapCenter Plug-ins Package for Linuxをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	2 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。

項目	要件
必要なソフトウェア パッケージ	Java 11 Oracle JavaおよびOpenJDK Javaを最新バージョンにアップグレードした場合は、<code>/var/opt/snapcenter/spl/etc/spl.properties</code>にある<code>JAVA_HOME</code>オプションが正しいJavaバージョンと正しいパスに設定されていることを確認する必要があります。 サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。

SnapCenter Plug-in for PostgreSQLのクレデンシャルの設定

SnapCenterは、クレデンシャルを使用してSnapCenterの処理を実行するユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、クラスターやWindowsファイルシステムでのデータ保護処理に使用する追加のクレデンシャルをそれぞれ作成する必要があります。

タスク概要

- Linuxホスト

Linuxホストにプラグインをインストールするには、クレデンシャルを設定する必要があります。

このクレデンシャルは、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo権限があるroot以外のユーザに対して設定します。

ベスト プラクティス: ホストをデプロイしてプラグインをインストールした後でも Linux の認証情報を作成できますが、ベスト プラクティスとしては、SVM を追加した後、ホストをデプロイしてプラグインをインストールする前に認証情報を作成します。

- Windowsホスト

プラグインのインストール前にWindowsクレデンシャルを設定する必要があります。

このクレデンシャルには、管理者権限（リモート ホストに対する管理者権限を含む）を設定する必要があります。

個々のリソース グループのクレデンシャルを設定する場合で、ユーザ名に完全なadmin権限が割り当てられていない場合は、少なくともリソース グループとバックアップの権限を割り当てる必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定] ページで、[資格情報] をクリックします。
3. *新規* をクリックします。
4. [Credential] ページで、クレデンシャルの設定に必要な情報を指定します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。
ユーザ名	認証に使用するユーザ名とパスワードを入力します。 - ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者またはSnapCenterプラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。ユーザ名フィールドの有効な形式は次のとおりです。 ◦ <i>NetBIOS</i>\ユーザ名 ◦ ドメイン<i>FQDN</i>\ユーザ名 - ローカル管理者（ワークグループの場合のみ） ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。ユーザー名フィールドの有効な形式は次のとおりです: <i>UserName</i> パスワードには二重引用符 (") やバッククォート (`) を使用しないでください。未満記号 (<) と感嘆符 (!) を組み合わせて使用したりしないでください。たとえば、<i>lessthan<!10</i>、<i>lessthan10<!</i>、バックティック `12 などです。
パスワード	認証に使用するパスワードを入力します。
Authentication Mode	使用する認証モードを選択します。
Use sudo privileges	非 root ユーザーの資格情報を作成する場合は、[sudo 権限を使用する] チェックボックスをオンにします。  Linuxユーザのみに該当します。

5. [OK]をクリックします。

クレデンシャルの設定が完了したら、必要に応じて[User and Access]ページでユーザやユーザ グループにク

レディンシャルを割り当てることができます。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、作成したグループ管理サービス アカウント (gMSA) を通じて、管理対象ドメイン アカウントからサービス アカウントのパスワードを自動管理できます。

開始する前に

- Windows Server 2016以降のドメイン コントローラが必要です。
- ドメインのメンバーであるWindows Server 2016以降のホストが必要です。

手順

1. KDSルート キーを作成し、gMSA内のオブジェクトごとに一意のパスワードを生成します。
2. 各ドメインについて、Windowsドメインコントローラから次のコマンドを実行します: Add-KDSRootKey -EffectiveImmediately
3. gMSAを作成して設定します。
 - a. 次の形式でユーザ グループ アカウントを作成します。

```
domainName\accountName$  
.. コンピュータ オブジェクトをグループに追加します。  
.. 作成したユーザ グループを使用してgMSAを作成します。
```

次に例を示します。

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 走る `Get-ADServiceAccount` サービス アカウントを確認するコマンド。
```

4. ホストでgMSAを設定します。
 - a. gMSAアカウントを使用するホストで、Windows PowerShell用のActive Directoryモジュールを有効にします。

これを行うには、PowerShellから次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. ホストを再起動します。
 - b. PowerShell コマンド プロンプトから次のコマンドを実行して、ホストに gMSA をインストールします。 `Install-AdServiceAccount <gMSA>`
 - c. 次のコマンドを実行して、gMSA アカウントを確認します。 `Test-AdServiceAccount <gMSA>`
5. ホスト上の設定済みgMSAに管理者権限を割り当てます。
 6. SnapCenter Serverで設定済みのgMSAアカウントを指定してWindowsホストを追加します。

SnapCenter Serverにより、選択したプラグインがホストにインストールされ、プラグインのインストール時には指定したgMSAがサービスのログオン アカウントとして使用されます。

SnapCenter Plug-in for PostgreSQLのインストール

ホストの追加とリモート ホストへのプラグイン パッケージのインストール

SnapCenterの[Add Host]ページを使用してホストを追加し、プラグイン パッケージをインストールする必要があります。プラグインは、自動的にリモート ホストにインストールされます。ホストの追加とプラグイン パッケージのインストールは、ホストごとに実行できます。

開始する前に

- SnapCenter Serverホストのオペレーティング システムがWindows 2019で、プラグイン ホストのオペレーティング システムがWindows 2022の場合は、次の手順を実行する必要があります。
 - Windows Server 2019 (OSビルド17763.5936) 以降にアップグレードする
 - Windows Server 2022 (OSビルド20348.2402) 以降にアップグレードする
- この処理は、SnapCenter Adminロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。

- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。
- メッセージ キュー サービスが実行中であることを確認する必要があります。
- ホストの管理については、管理に関するドキュメントを参照してください。
- グループ管理サービス アカウント（gMSA）を使用する場合は、管理者権限でgMSAを設定する必要があります。

"Windows Server 2016 以降で PostgreSQL 用のグループ管理サービス アカウントを構成する"

タスク概要

- SnapCenter Serverをプラグイン ホストとして別のSnapCenter Serverに追加することはできません。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. 上部の*管理対象ホスト*タブが選択されていることを確認します。
3. *[追加]*をクリックします。
4. [Hosts]ページで、次の操作を実行します。

フィールド	操作
ホストタイプ	ホストのタイプを選択します。 • Windows • Linux  Plug-in for PostgreSQL は、PostgreSQLクライアント ホ ストにインストールされます。 このホストは、Windowsシステ ムでもLinuxシステムでもかまい ません。
ホスト名	通信ホスト名を入力します。ホストの完全修飾ドメ イン名（FQDN）またはIPアドレスを入力しま す。SnapCenterが機能するためには、DNSが適切 に設定されている必要があります。そのた め、FQDNを入力することを推奨します。

フィールド	操作
Credentials	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。このクレデンシャルには、リモート ホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。  クレデンシャルの認証モードは、[Add Host]ウィザードで指定するホスト タイプによって決まります。

5. [Select Plug-ins to Install]セクションで、インストールするプラグインを選択します。

REST APIを使用してPlug-in for PostgreSQLをインストールする場合は、バージョンを3.0として渡す必要があります。例：PostgreSQL:3.0

6. (オプション) [その他のオプション] をクリックします。

フィールド	操作
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。デフォルトのポート番号は8145です。SnapCenter Serverがカスタム ポートにインストールされている場合は、そのポート番号がデフォルト ポートとして表示されます。  プラグインを手動でインストールしてカスタム ポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理が失敗します。
Installation Path	Plug-in for PostgreSQLは、PostgreSQLクライアント ホストにインストールされます。このホストは、WindowsシステムでもLinuxシステムでもかまいません。 • Windows 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは C:\Program Files\ NetApp\ SnapCenterです。必要に応じて、パスをカスタマイズできます。 • Linux 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは /opt/ NetApp/snapcenter です。必要に応じて、パスをカスタマイズできます。

フィールド	操作
Skip preinstall checks	プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスをオンにします。
クラスター内のすべてのホストを追加する	すべてのクラスターノードを追加するには、このチェックボックスをオンにします。
Use group Managed Service Account (gMSA) to run the plug-in services	Windowsホストで、グループ管理サービスアカウント (gMSA) を使用してプラグイン サービスを実行する場合は、このチェックボックスをオンにします。  gMSA名をdomainName\accountName\$の形式で指定します。  gMSAは、SnapCenter Plug-in for Windowsサービスのログオン サービスアカウントとしてのみ使用されます。

7. *送信*をクリックします。

[Skip prechecks]チェックボックスを選択していない場合、プラグインをインストールするための要件をホストが満たしているかどうかを検証するためにホストが検証されます。ディスクスペース、RAM、PowerShellのバージョン、.NETのバージョン、場所（Windowsプラグインの場合）、Javaのバージョン（Linuxプラグインの場合）が最小要件に照らして検証されます。最小要件を満たしていない場合、対応するエラーまたは警告メッセージが表示されます。

エラーがディスクスペースまたはRAMに関連している場合は、C:\Program Files\NetApp\SnapCenter\WebAppにあるweb.configファイルを更新してデフォルト値を変更できます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。



HAのセットアップでweb.configファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. ホストタイプがLinuxの場合は、フィンガープリントを確認し、[確認して送信]をクリックします。

クラスターセットアップでは、クラスター内の各ノードのフィンガープリントを検証する必要があります。



前述の手順で同じホストがSnapCenterに追加され、フィンガープリントが確認された場合でも、フィンガープリントの検証は必須です。

9. インストールの進捗状況を監視します。

- Windows プラグインの場合、インストールおよびアップグレード ログは次の場所にあります:
C:\Windows\SnapCenter plugin\Install<JOBID>_

- Linux プラグインの場合、インストール ログは次の場所にあります:
`/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log_`、アップグレード ログは次の場所にあります: `/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade<JOBID>.log_`

コマンドレットを使用した複数のリモート ホストへの**SnapCenter Plug-ins Package for Linux / Windows**のインストール

Install-SmHostPackage PowerShellコマンドレットを使用すると、複数のホストに**SnapCenter Plug-ins Package for Linux / Windows**を同時にインストールできます。

開始する前に

プラグイン パッケージをインストールする各ホストに対するローカル管理者権限を持つドメイン ユーザとして、SnapCenterにログインしておく必要があります。

手順

1. PowerShellを起動します。
2. SnapCenter Serverホストで、**Open-SmConnection**コマンドレットを使用してセッションを確立し、クレデンシャルを入力します。
3. **Install-SmHostPackage**コマンドレットと必要なパラメータを使用して、複数のホストにプラグインをインストールします。

コマンドレットで使用できるパラメータとその説明に関する情報は、***Get-Help command_name*** を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、**-skipprecheck**オプションを使用できます。

4. リモート インストールのクレデンシャルを入力します。

コマンドライン インターフェイスを使用した**Linux**ホストへの**SnapCenter Plug-in for PostgreSQL**のインストール

SnapCenter Plug-in for PostgreSQL クラスタは、SnapCenterユーザ インターフェイス (UI) を使用してインストールする必要があります。SnapCenter UIからのプラグインのリモート インストールが許可されていない環境では、コマンドライン インターフェイス (CLI) を使用して、コンソール モードまたはサイレント モードで**Plug-in for PostgreSQL**クラスタをインストールできます。

開始する前に

- **Plug-in for PostgreSQL**クラスタは、PostgreSQLクライアントがあるLinuxホストごとにインストールする必要があります。
- **SnapCenter Plug-in for PostgreSQL**クラスタをインストールするLinuxホストは、依存するソフトウェア、クラスタ、オペレーティング システムの要件を満たしている必要があります。

サポートされる構成に関する最新の情報については、**Interoperability Matrix Tool (IMT)** を参照してください。

["NetApp Interoperability Matrix Tool"](#)

- SnapCenter Plug-in for PostgreSQL クラスタは、SnapCenter Plug-ins Package for Linuxに含まれています。SnapCenter Plug-ins Package for Linuxをインストールする前に、SnapCenterをWindowsホストにインストールしておく必要があります。

手順

1. SnapCenter Plug-ins Package for Linuxのインストール ファイル (snapcenter_linux_host_plugin.bin) をC:\ProgramData\NetApp\SnapCenter\Package RepositoryからPlug-in for PostgreSQLをインストールするホストにコピーします。

このパスには、SnapCenter Serverがインストールされているホストからアクセスできます。

2. コマンド プロンプトから、インストール ファイルをコピーしたディレクトリに移動します。
3. プラグインをインストールします。

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address  
-DSERVER_HTTPS_PORT=port_number_for_server
```

- -DPORT は SMCORE HTTPS 通信ポートを指定します。
- -DSERVER_IP は、 SnapCenter Server の IP アドレスを指定します。
- -DSERVER_HTTPS_PORT は、 SnapCenter Server の HTTPS ポートを指定します。
- -DUSER_INSTALL_DIR は、Linux 用のSnapCenterプラグイン パッケージをインストールするディレクトリを指定します。
- DINSTALL_LOG_NAME はログ ファイルの名前を指定します。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146  
-DUSER_INSTALL_DIR=/opt  
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log  
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. <インストール ディレクトリ>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties ファイルを編集し、PLUGINS_ENABLED = PostgreSQL:3.0 パラメータを追加します。
5. Add-Smhostコマンドレットと必要なパラメータを使用して、SnapCenter Serverにホストを追加します。

コマンドで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

Plug-in for PostgreSQLのインストール ステータスの監視

[Jobs]ページを使用して、SnapCenterプラグイン パッケージのインストールの進捗状況を監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、プラグインのインストール操作のみがリストされるようにリストをフィルタリングするには、次の手順を実行します。
 - a. *フィルター*をクリックします。
 - b. オプション：開始日と終了日を指定します。
 - c. [タイプ] ドロップダウン メニューから、[プラグインのインストール] を選択します。
 - d. [Status]ドロップダウン メニューから、インストールのステータスを選択します。
 - e. *適用*をクリックします。
4. インストール ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

CA証明書の設定

CA証明書CSRファイルの生成

証明書署名要求（CSR）を生成し、生成したCSRを使用して認証局（CA）から取得した証明書をインポートできます。証明書には秘密キーが関連付けられます。

CSRはエンコードされたテキストのブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。



CA 証明書の RSA キーの長さは最低 3072 ビットである必要があります。

CSRを生成するための情報については、["CA証明書CSRファイルの生成方法"](#)。



ドメイン (*.domain.company.com) またはシステム (machine1.domain.company.com) の CA 証明書を所有している場合は、CA 証明書 CSR ファイルの生成をスキップできます。SnapCenterを使用して、既存のCA証明書を導入できます。

クラスタ構成の場合、クラスタ名（仮想クラスタFQDN）と、それぞれのホスト名がCA証明書に記載されている必要があります。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。ワイルドカード証明書 (*.domain.company.com) の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenter ServerとWindowsホスト プラグインにCA証明書をインポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
4. コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書 をクリックします。
5. 「信頼されたルート証明機関」フォルダを右クリックし、[すべてのタスク] > [インポート] を選択して、インポート ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*次へ*をクリックします。
インポート ファイル形式	変更せずに、[次へ] をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、[次へ] をクリックします。
証明書のインポート ウィザードの完了	概要を確認し、[完了] をクリックしてインポートを開始します。



インポートする証明書は秘密キーとバンドルされている必要があります (サポートされている形式は **.pfx**、**.p12**、および ***.p7b** です)。

7. 「個人用」フォルダに対して手順5を繰り返します。

CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための16進数の文字列です。サムプリントは、サムプリント アルゴリズムを使用して証明書の内容から計算されます。

手順

1. GUIで次の手順を実行します。
 - a. 証明書をダブルクリックします。
 - b. [証明書] ダイアログボックスで、[詳細] タブをクリックします。

- c. フィールドのリストをスクロールして、「拇印」をクリックします。
- d. ボックスから16進数の文字をコピーします。
- e. 16進数の間のスペースを削除します。

たとえば、拇印が「a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b」の場合、スペースを削除すると「a909502dd82ae41433e6f83886b00d4277a32a7b」になります。

2. PowerShellで、次の手順を実行します。

- a. 次のコマンドを実行して、インストールされている証明書のサムプリントを表示し、最近インストールされた証明書をサブジェクト名で識別します。

```
Get-ChildItem -Path 証明書:\LocalMachine\My
```

- b. サムプリントをコピーします。

Windowsホスト プラグイン サービスでのCA証明書の設定

インストールされているデジタル証明書をアクティブ化するには、Windowsホスト プラグイン サービスを使用してCA証明書を設定する必要があります。

SnapCenter Serverと、CA証明書がすでに導入されているすべてのプラグイン ホストで、次の手順を実行します。

手順

- 1. 次のコマンドを実行して、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例えば：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

． 次のコマンドを実行して、新しくインストールした証明書をWindowsホスト プラグイン サービスとバインドします。

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

例えば：


```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

LinuxホストでのSnapCenter PostgreSQL Plug-insサービスのCA証明書の設定

インストールされたデジタル証明書をアクティブ化するには、SnapCenterプラグインサービスを使用して、プラグイン キーストアとその証明書のパスワードを管理し、CA証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、`/opt/NetApp/snapcenter/scc/etc`にあるファイル「`keystore.jks`」を使用します。

プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

キー「`KEYSTORE_PASS`」に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks  
. キーストア内の秘密キー  
エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

`agent.properties` ファイルのキー `KEYSTORE_PASS` も同様に更新します。

3. パスワードを変更したら、サービスを再起動します。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは同じである必要があります。

ルート証明書または中間証明書をプラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグイン キーストアが含まれるフォルダーに移動します: /opt/ NetApp/snapcenter/scc/etc。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. ルート証明書か中間証明書を追加します。

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

・
ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。
。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアに**CA**署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグイン キーストア /opt/ NetApp/snapcenter/scc/etc が含まれるフォルダーに移動します。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

6. キーストアに追加された新しいCA証明書に対応するエイリアスが、キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのプラグイン キーストア パスワードは、agent.properties ファイルのキー KEYSTORE_PASS の値です。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

・ CA 証明書のエイリアス名が長く、スペースや特殊文字（「*」、「」）が含まれている場合は、エイリアス名を単純な名前に変更します。

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

・ agent.properties ファイルの CA 証明書からエイリアス名を設定します。

この値を、キー SCC_CERTIFICATE_ALIAS に対して更新します。

8. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

プラグインの証明書失効リスト（CRL）を構成する

タスク概要

- ・ SnapCenter プラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- ・ SnapCenter プラグインの CRL ファイルのデフォルト ディレクトリは、「opt/NetApp/snapcenter/scc/etc/crl」です。

手順

1. キー CRL_PATH に対して、agent.properties ファイルのデフォルト ディレクトリを変更、更新できます。

このディレクトリには、複数の CRL ファイルを格納できます。受信する証明書については、それぞれの CRL に対して検証が行われます。

Windows ホストでの SnapCenter PostgreSQL Plug-ins サービスの CA 証明書の設定

インストールされたデジタル証明書をアクティブ化するには、SnapCenter プラグイン サービスを使用して、プラグイン キーストアとその証明書のパスワードを管理し、CA 証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc にあるファイル keystore.jks を使用します。

プラグインキーストアのパスワードと使用中の CA 署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

これはキー _KEYSTORE_PASS_ に対応する値です。

2. キーストアのパスワードを変更します。

`keytool -storepasswd -keystore keystore.jks`



Windowsコマンド プロンプトで「keytool」 コマンドが認識されない場合は、keytoolコマンドを完全なパスに置き換えます。

`C:\Program Files\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks`

3. キーストア内の秘密キー エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

`keytool -keypasswd -alias "証明書内のエイリアス名" -keystore keystore.jks`

`agent.properties` ファイルのキー `KEYSTORE_PASS` も同様に更新します。

4. パスワードを変更したら、サービスを再起動します。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは同じである必要があります。

ルート証明書または中間証明書をプラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_` に移動します。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

`keytool -list -v -keystore keystore.jks`

4. ルート証明書か中間証明書を追加します。

`keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks`

5. ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアにCA署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_` に移動します。
2. ファイル `keystore.jks` を見つけます。

3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

6. キーストアに追加された新しいCA証明書に対応するエイリアスが、キーストアに含まれていることを確認します。

7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのプラグイン キーストア パスワードは、agent.properties ファイルのキー KEYSTORE_PASS の値です。

```
keytool -keypasswd -alias "CA証明書のエイリアス名" -keystore keystore.jks
```

8. agent.properties ファイル内の CA 証明書からエイリアス名を設定します。

この値を、キーSCC_CERTIFICATE_ALIASに対して更新します。

9. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

SnapCenterプラグインの証明書失効リスト（CRL）を構成する

タスク概要

- 関連するCA証明書の最新のCRLファイルをダウンロードするには、["SnapCenter CA証明書の証明書失効リストファイルを更新する方法"](#)。
- SnapCenterプラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- SnapCenterプラグインの CRL ファイルのデフォルト ディレクトリは、'C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\ etc\crl' です。

手順

1. キー CRL_PATH に対して、agent.properties ファイル内のデフォルト ディレクトリを変更および更新できます。
2. このディレクトリには、複数のCRLファイルを格納できます。

受信する証明書については、それぞれのCRLに対して検証が行われます。

プラグインのCA証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインでCA証明書の検証を有効にする必要があります。

開始する前に

- 実行 `Set-SmCertificateSettings` コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- `Get-SmCertificateSettings` を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. プラグイン ホストを1つまたは複数選択します。
4. *その他のオプション* をクリックします。
5. *証明書の検証を有効にする* を選択します。

終了後の操作

[Managed Hosts] タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Server とプラグイン ホスト間の接続のステータスを示します。

- *  * は、CA 証明書が有効になっていないか、プラグイン ホストに割り当てられていないことを示します。
- *  * は CA 証明書が正常に検証されたことを示します。
- *  * は、CA 証明書を検証できなかったことを示します。
- *  * は接続情報を取得できなかったことを示します。



ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

データ保護の準備

SnapCenter Plug-in for PostgreSQLを使用するための前提条件

ユーザがSnapCenter Plug-in for PostgreSQLを使用するためには、SnapCenter管理者が事前にSnapCenter Serverをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter Serverをインストールして設定します。
- SnapCenter Serverにログインします。
- SnapCenter環境を設定するために、必要に応じて、ストレージ システム接続を追加し、クレデンシャルを作成します。
- LinuxホストまたはWindowsホストにJava 11をインストールします。

Javaパスは、ホスト マシンの環境パス変数で設定する必要があります。

- バックアップ レプリケーションが必要である場合は、SnapMirrorとSnapVaultをセットアップします。

PostgreSQLの保護におけるソース、リソース グループ、ポリシーの使用方法

SnapCenterを使用する前に、実行するバックアップ、クローニング、リストアの各処理に関連する基本的な概念を理解しておく役立ちます。ここでは、これらの処理で扱うリソース、リソース グループ、およびポリシーについて説明します。

- リソースとは、一般にはSnapCenterでバックアップまたはクローニングするPostgreSQLクラスタのことです。
- SnapCenterリソース グループは、ホスト上のリソースの集まりです。

リソース グループに対して処理を実行すると、リソース グループに指定したスケジュールに従って、リソース グループに定義されているリソースに対して処理が実行されます。

単一のリソースまたはリソース グループをオンデマンドでバックアップすることができます。また、スケジュールされたバックアップを単一リソースおよびリソース グループに対して実行することもできます。

- ポリシーは、バックアップ頻度、レプリケーション、スクリプトといった、データ保護処理の特性を指定するものです。

リソース グループを作成するときに、そのグループに対して1つ以上のポリシーを選択します。単一リソースに対してオンデマンドでバックアップを実行するときにもポリシーを選択できます。

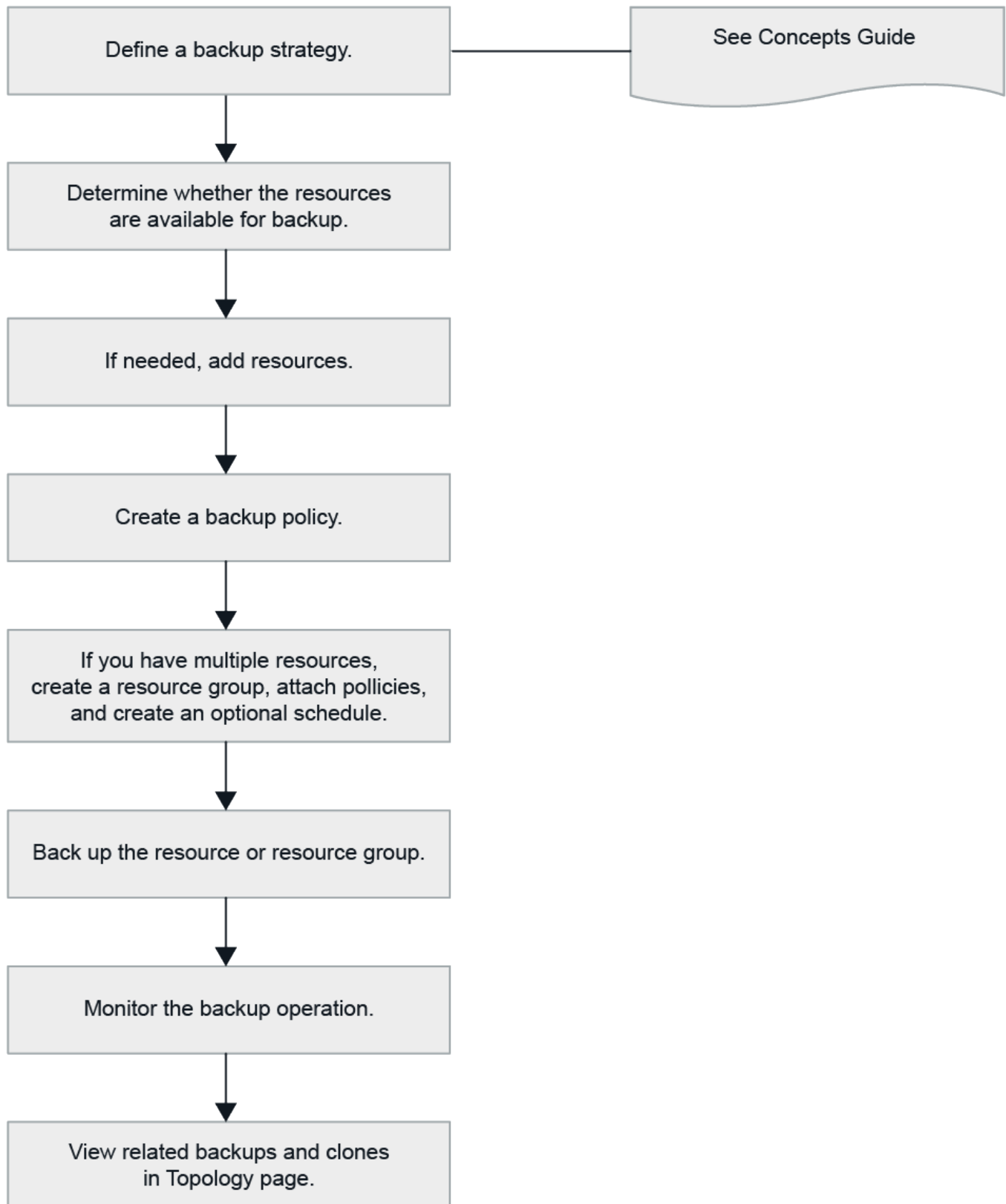
リソース グループでは、保護する対象と保護するタイミング（日時）を定義できます。ポリシーでは、保護する方法を定義できます。たとえば、すべてのクラスタをバックアップする場合は、ホストのすべてのクラスタを含むリソース グループを作成します。このリソース グループに、日次ポリシーと毎時ポリシーの2つのポリシーを適用します。リソース グループを作成してポリシーを適用する際に、フル バックアップを1日1回実行するようにリソース グループを設定できます。

PostgreSQLリソースのバックアップ

PostgreSQLリソースのバックアップ

リソース（クラスタ）またはリソース グループのバックアップを作成することができます。バックアップのワークフローには、計画、バックアップするクラスタの特定、バックアップ ポリシーの管理、リソース グループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

次のワークフローは、バックアップ処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトでを使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。<https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html>["SnapCenterソフトウェア コマンドレット リファレンス ガイド"^]。

クラスタの自動的検出

リソースとは、SnapCenterで管理するLinuxホスト上のPostgreSQLクラスタです。使用できるPostgreSQLクラスタを検出したあとに、それらのリソースをリソース グループに追加してデータ保護処理を実行できます。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の作成などのタスクを事前に完了しておく必要があります。
- SnapCenter Plug-in for PostgreSQLでは、RDM / VMDK仮想環境にあるリソースの自動検出がサポートされていません。

タスク概要

- プラグインをインストールすると、そのLinuxホスト上のすべてのクラスタが自動検出されて[Resources]ページに表示されます。
- 自動検出されるのはクラスタのみです。

自動検出されたリソースを変更または削除することはできません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから PostgreSQL 用プラグインを選択します。
2. [Resources]ページで、[View]リストからリソース タイプを選択します。
3. (オプション) をクリック 、ホスト名を選択します。

をクリックします  フィルター パネルを閉じます。

4. ホスト上で利用可能なリソースを検出するには、[リソースの更新] をクリックします。

リソースは、リソース タイプ、ホスト名、関連するリソース グループ、バックアップ タイプ、ポリシー、全体的なステータスなどの情報とともに表示されます。

- クラスタがNetAppストレージにあって保護されていない場合は、[Overall Status]列に「Not protected」と表示されます。
- クラスタがNetAppストレージ システム上にあって保護されており、バックアップ処理が実行されていない場合は、[Overall Status]列に「Backup not run」と表示されます。それ以外の場合は、前回のバックアップ ステータスに基づいて、ステータスが「バックアップに失敗しました」または「バックアップに成功しました」に変わります。



SnapCenterの外部でクラスタの名前が変更された場合は、リソースを更新する必要があります。

手動でのプラグイン ホストへのリソースの追加

自動検出はWindowsホストではサポートされていません。PostgreSQLクラスタ リソースは手動で追加する必要があります。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の設定などのタスクを完了しておく必要があります。

タスク概要

自動検出は、次の構成ではサポートされていません。

- RDMおよびVMDKレイアウト

手順

1. 左側のナビゲーション ペインで、ドロップダウン リストからSnapCenter Plug-in for Postgresql を選択し、[リソース] をクリックします。
2. [リソース] ページで、[Postgresql リソースの追加] をクリックします。
3. [Provide Resource Details]ページで、次の操作を実行します。

フィールド	操作
Name	クラスタ名を指定します。
Host Name	ホスト名を入力します。
タイプ	[cluster]を選択します。
Instance	クラスタの親であるインスタンスの名前を指定します。
Credentials	クレデンシャルを選択するか、クレデンシャルの情報を追加します。 これはオプションです。

4. [ストレージ フットプリントの提供] ページで、ストレージ タイプを選択し、1 つ以上のボリューム、LUN、および qtree を選択して、[保存] をクリックします。

オプション：をクリックすることもできます  アイコンをクリックして、他のストレージ システムからボリューム、LUN、qtree を追加します。
5. オプション: リソース設定ページで、Windowsホスト上のリソースの場合は、PostgreSQLプラグインのカスタムキーと値のペアを入力します。
6. 概要を確認し、[完了] をクリックします。

クラスタは、ホスト名、関連するリソース グループとポリシー、全体的なステータスなどの情報とともに表示されます。

リソースへのアクセスをユーザに許可する場合は、ユーザにリソースを割り当てる必要があります。これにより、ユーザは、自身に割り当てられたアセットに対して、権限のある処理を実行できるようになります。

"ユーザまたはグループの追加と、ロールとアセットの割り当て"

終了後の操作

- クラスタを追加したあとで、PostgreSQLクラスタの詳細を変更できます。
- SnapCenter 5.0から移行されたリソース（表領域とクラスタ）は、SnapCenter 6.0ではPostgreSQLクラスタ タイプとしてタグ付けされます。
- SnapCenter 5.0 以前から移行された手動で追加されたリソースを変更する場合は、カスタム キー値ペアのリソース設定 ページで次の操作を行います。
 - 名前 フィールドに「PORT」という用語を指定します。
 - 値 フィールドにポート番号を指定します。

PostgreSQLのバックアップ ポリシーの作成

SnapCenterを使用してPostgreSQLリソースをバックアップする前に、バックアップ対象のリソースまたはリソース グループのバックアップ ポリシーを作成する必要があります。バックアップ ポリシーとは、バックアップをどのように管理し、スケジューリングし、保持するかを定める一連のルールです。

開始する前に

- バックアップ戦略を定義しておく必要があります。

詳細については、PostgreSQLクラスタのデータ保護戦略の定義に関する説明を参照してください。

- SnapCenterのインストール、ホストの追加、ストレージ システム接続の作成、リソースの追加などのタスクを実行して、データ保護の準備をしておく必要があります。
- ユーザがSnapshotをミラーまたはバックアップにレプリケートする場合は、ソース ボリュームとデスティネーション ボリューム両方のSVMをSnapCenter管理者がユーザに割り当てる必要があります。

ポリシーで、レプリケーション、スクリプト、アプリケーション設定を指定することもできます。それらのオプションを指定しておくことで、別のリソース グループにポリシーを再利用して時間を節約することができます。

タスク概要

- SnapLock
 - [Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで指定した保持日数以下にする必要があります。
 - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、ポリシーで指定した数よりも多くのSnapshotが保持される可能性があります。
 - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[ポリシー]をクリックします。

3. *新規*をクリックします。
4. 「名前」ページで、ポリシー名と詳細を入力します。
5. [Policy type]ページで、次の手順を実行します。
 - a. ストレージ タイプを選択します。
 - b. カスタム バックアップ設定 セクションで、キーと値の形式でプラグインに渡す必要がある特定のバックアップ設定を指定します。

プラグインに渡すキーと値のペアを複数指定することができます。

6. 「バックアップとレプリケーション」ページで、次のアクションを実行します。

- a. オンデマンド、時間別、日次、週次、または*月次*を選択して、スケジュールの頻度を指定します。



リソース グループを作成する際に、バックアップ処理のスケジュール（開始日、終了日、頻度）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソース グループを作成できますが、各ポリシーに異なるバックアップ スケジュールを割り当てることができます。



午前 2 時にスケジュールを設定した場合、夏時間 (DST) 中はスケジュールは実行されません。

- a. スナップショット設定セクションで、バックアップ タイプ ページで選択したバックアップ タイプとスケジュール タイプの保持設定を指定します。

状況	操作
特定の数のSnapshotを保持	*保持するコピー*を選択し、保持するスナップショットの数を指定します。 Snapshotの数が指定した数を超えると、古いものから順にSnapshotが削除されます。 SnapVaultレプリケーションを有効にする場合は、保持数を2以上に設定する必要があります。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。 最大保持値は 1018 です。保持期間がONTAPバージョンでサポートされている値よりも高い値に設定されている場合、バックアップは失敗します。

状況	操作
Snapshotを特定の日数だけ保持	*コピーの保持期間*を選択し、スナップショットを削除する前に保持する日数を指定します。
スナップショットコピーのロック期間	スナップショット コピーのロック期間 を選択し、日、月、または年を指定します。 SnapLock保持期間は100年未満にする必要があります。

7. ポリシーラベルを選択します。



リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしなくても実行できます。

8. [セカンダリ レプリケーション オプションの選択] セクションで、次のセカンダリ レプリケーション オプションの 1 つまたは両方を選択します。

フィールド	操作
ローカル スナップショット コピーを作成した後、 SnapMirror を更新します	別のボリュームにバックアップ セットのミラー コピーを作成する場合（SnapMirrorレプリケーション）は、このフィールドを選択します。 ONTAPの保護関係のタイプがミラーとバックアップの場合、このオプションのみを選択すると、プライマリで作成されたSnapshotがデスティネーションに転送されませんが、デスティネーションのリストに表示されます。このスナップショットを復元操作を実行するために宛先から選択すると、次のエラー メッセージが表示されます: 選択したボールド/ミラー バックアップにはセカンダリ ロケーションは使用できません。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。 トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 見る"トポロジページでPostgreSQLリソース関連のバックアップとクローンを表示します。"。

フィールド	操作
ローカルスナップショットコピーを作成した後、 SnapVault を更新します	ディスクツーディスクのバックアップ レプリケーション（SnapVaultバックアップ）を実行する場合は、このオプションを選択します。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 SnapLock がSnapLock Vault と呼ばれるONTAPのセカンダリにのみ設定されている場合、[トポロジ] ページの [更新] ボタンをクリックすると、ONTAPから取得されたセカンダリのロック期間が更新されます。 SnapLock Vault の詳細については、「Vault の保存先でスナップショットを WORM にコミットする」を参照してください。 見る"トポロジページでPostgreSQLリソース関連のバックアップとクローンを表示します。"。
エラー再試行回数	処理が停止されるまでに試行できるレプリケーションの最大回数を入力します。



セカンダリ ストレージでSnapshotの上限に達しないように、ONTAPでセカンダリ ストレージのSnapMirror保持ポリシーを設定する必要があります。

9. 概要を確認し、[完了] をクリックします。

リソース グループの作成とポリシーの適用

リソース グループはコンテナであり、バックアップして保護するリソースをここに追加する必要があります。リソース グループを使用することで、特定のアプリケーションに関連するすべてのデータを同時にバックアップできます。リソース グループはいずれのデータ保護ジョブにも必要になります。リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義することも必要です。

タスク概要

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。

2. [リソース] ページで、[新しいリソース グループ] をクリックします。

3. [Name] ページで、次の操作を実行します。

フィールド	操作
Name	リソース グループの名前を入力します。  リソース グループ名は250文字以内で指定する必要があります。
Tags	リソース グループを検索しやすくするために、ラベルを入力します。 たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。
Use custom name format for snapshot copy	Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。 たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

4. [リソース] ページで、[ホスト] ドロップダウン リストからホスト名を選択し、[リソース タイプ] ドロップダウン リストからリソース タイプを選択します。

画面の情報がフィルタリングされます。

5. *利用可能なリソース*セクションからリソースを選択し、右矢印をクリックして*選択したリソース*セクションに移動します。

6. [Application Settings] ページで、次の操作を実行します。

a. 追加のバックアップ オプションを設定するには、[バックアップ] 矢印をクリックします。

整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for Consistency Group snapshot operation to complete	スナップショット操作が完了するまでの待機時間を指定するには、「緊急」、「中」、または「緩和」を選択します。 [Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。

フィールド	操作
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

+

- *スクリプト*矢印をクリックし、静止、スナップショット、および静止解除操作の事前および事後コマンドを入力します。障害の発生時に終了前に実行するプリコマンドも入力できます。
- *カスタム構成*矢印をクリックし、このリソースを使用するすべてのデータ保護操作に必要なカスタムのキーと値のペアを入力します。

パラメータ	設定	説明
ARCHIVE_LOG_ENABLE	(Y / N)	アーカイブ ログ管理を有効にし、アーカイブ ログを削除します。
ARCHIVE_LOG_RETENTION	number_of_days	アーカイブ ログを保持する日数を指定します。 この設定は、NTAP_SNAPSHOT_RETENTIONS 以上である必要があります。
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブ ログが含まれるディレクトリへのパスを指定します。

パラメータ	設定	説明
ARCHIVE_LOG_EXT	file_extension	アーカイブ ログ ファイルの拡張子の長さを指定します。 たとえば、アーカイブ ログが log_backup_0_0_0_0.161518551942 9 で、file_extension 値が 5 の場合、ログの拡張子は 5 桁、つまり 16151 になります。
ARCHIVE_LOG_RECURSIVE_SE ARCH	(Y / N)	サブディレクトリ内のアーカイブ ログの管理を有効にします。 アーカイブ ログがサブディレクトリの下にある場合は、このパラメータを使用する必要があります。



カスタムのキーと値のペアは、PostgreSQL Linuxプラグイン システムではサポートされますが、一元化されたWindowsプラグインとして登録されたPostgreSQLクラスタではサポートされません。

- c. スナップショット コピー ツール の矢印をクリックして、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する（このオプションはLinuxリソースには適用されません）	ファイル システムの一貫性を備えたSnapCenter * を選択します。
SnapCenterでストレージ レベルのSnapshotを作成する	ファイル システムの整合性のないSnapCenter * を選択します。
Snapshotを作成するためにホストで実行するコマンドを入力する	*その他*を選択し、スナップショットを作成するためにホスト上で実行するコマンドを入力します。

7. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます  。

ポリシーが[Configure schedules for selected policies]セクションのリストに表示されます。

- b. スケジュールの設定列で*をクリックします。  * 設定するポリシーの。
- c. ポリシー *policy_name* のスケジュールの追加ダイアログ ボックスでスケジュールを構成し、[OK] をクリックします。

*policy_name*は、選択したポリシーの名前です。

構成されたスケジュールは、「適用されたスケジュール」列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP サーバーは、設定 > グローバル設定 で設定する必要があります。

9. 概要を確認し、[完了] をクリックします。

ASA r2 システム上の PostgreSQL リソースのリソース グループを作成し、二次保護を有効にする

ASA r2 システム上にあるリソースを追加するには、リソース グループを作成する必要があります。リソース グループの作成時にセカンダリ保護をプロビジョニングすることもできます。

開始する前に

- ONTAP 9.x リソースとASA r2 リソースの両方を同じリソース グループに追加していないことを確認する必要があります。
- ONTAP 9.x リソースとASA r2 リソースの両方を含むデータベースが存在しないことを確認する必要があります。

タスク概要

- 二次保護は、ログインしたユーザーに **SecondaryProtection** 機能が有効になっているロールが割り当てられている場合にのみ使用できます。
- セカンダリ保護を有効にすると、プライマリおよびセカンダリ整合性グループの作成中にリソース グループはメンテナンス モードになります。プライマリおよびセカンダリのコンシステンシー グループが作成されると、リソース グループのメンテナンス モードが解除されます。
- SnapCenter はクローン リソースの二次保護をサポートしていません。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name]ページで、次の操作を実行します。
 - a. [Name]フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag]フィールドに1つ以上のラベルを入力します。

たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

- c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

たとえば、`customtext_resource group_policy_hostname`や`resource group_hostname`などの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- d. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。



必要に応じて、プレフィックスを含め、アプリケーションで設定されたのと同じ宛先を使用する必要があります。

4. [リソース] ページで、[ホスト] ドロップダウン リストからデータベース ホスト名を選択します。



[Available Resources]セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources]のリストには表示されません。

5. [使用可能なリソース] セクションからASA r2 リソースを選択し、[選択したリソース] セクションに移動します。
6. アプリケーション設定ページで、バックアップ オプションを選択します。
7. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックし  てポリシーを作成することもできます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、  をクリックします。
- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 選択したポリシーに対して二次保護が有効になっている場合は、「二次保護」 ページが表示されるので、次の手順を実行する必要があります。

- a. レプリケーション ポリシーのタイプを選択します。



同期レプリケーション ポリシーはサポートされていません。

- b. 使用する整合性グループのサフィックスを指定します。

- c. [宛先クラスタ] および [宛先 SVM] ドロップダウンから、使用するピア クラスタと SVM を選択します。



クラスタと SVM のピアリングはSnapCenterではサポートされていません。クラスタと SVM のピアリングを実行するには、System Manager またはONTAP CLI を使用する必要があります。



リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは [セカンダリ保護リソース] セクションに表示されます。

1. [Verification] ページで、次の手順を実行します。

- a. ロケータのロード をクリックして、 SnapMirrorまたはSnapVaultボリュームをロードし、セカンダリストレージで検証を実行します。
- b. クリック  ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で をクリックします。
- c. [Add Verification Schedules policy_name] ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

- d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証] を選択します。
- e. [OK] をクリックします。

設定した検証スケジュールが、[Applied Schedules] 列にリストされます。

2. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtptServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

3. 概要を確認し、[完了] をクリックします。

PostgreSQL用のPowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成

PowerShellコマンドレットを使用してPostgreSQLクラスタのバックアップ、リストア、クローニングを行う前に、Storage Virtual Machine (SVM) 接続とクレデンシャルを作成する必要があります。

開始する前に

- PowerShellコマンドレットを実行できるようにPowerShell環境を準備しておく必要があります。
- ストレージ接続を作成するには、Infrastructure Adminロールの権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

ストレージ システム接続の追加中は、ホスト プラグインのインストールが進行中であってはなりません。ホスト キャッシュが更新されず、 SnapCenter GUI にクラスタのステータスが「バックアップに使用できません」または「NetAppストレージ上にありません」と表示される可能性があるためです。

- ストレージ システムの名前は一意である必要があります。

SnapCenterでは、別々のクラスタに属している場合でも、複数のストレージ システムに同じ名前を付けることはサポートされません。SnapCenterでサポートする各ストレージ システムには、一意な名前とデータLIFの一意なIPアドレスが必要です。

手順

1. Open-SmConnectionコマンドレットを使用して、PowerShell Core接続セッションを開始します。

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

2. Add-SmStorageConnectionコマンドレットを使用して、ストレージ システムへの新しい接続を作成します。

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Add-SmCredentialコマンドレットを使用して、新しいクレデンシャルを作成します。

この例は、Windowsクレデンシャルを使用してFinanceAdminという名前の新しいクレデンシャルを作成する方法を示しています。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. SnapCenter ServerにPostgreSQL通信ホストを追加します。

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName FinanceAdmin -PluginCode PostgreSQL
```

5. パッケージとSnapCenter Plug-in for PostgreSQLをホストにインストールします。

Linux :

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode PostgreSQL
```

Windows :

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode PostgreSQL -FilesystemCode scw -RunAsName FinanceAdmin
```

6. SQLLIBのパスを設定します。

Windows の場合、PostgreSQL プラグインは SQLLIB フォルダのデフォルト パス「C:\Program Files\IBM\SQLLIB\BIN」を使用します。

デフォルト パスを上書きする場合は、次のコマンドを使用します。

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

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

PostgreSQLのバックアップ

どのリソース グループにもまだ含まれていないリソースは、[Resources]ページからバックアップすることができます。

開始する前に

- バックアップ ポリシーを作成しておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。
- Snapshotコピーベースのバックアップ処理の場合は、すべてのテナント クラスタが有効でアクティブであることを確認してください。
- 休止、Snapshot、および休止解除の処理を実行するプリコマンドとポストコマンドの場合は、プラグイン

ホストで次のパスから使用できるコマンド リストにコマンドがあるかどうかを確認する必要があります。

- Windows ホスト上のデフォルトの場所: `C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux ホスト上のデフォルトの場所: `/opt/ NetApp/ snapcenter/ scc/ etc/ allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. リソース ページで、リソース タイプに基づいて 表示 ドロップダウン リストからリソースをフィルターします。

を選択 、ホスト名とリソース タイプを選択して、リソースをフィルターします。次に選択できます  フィルター パネルを閉じます。

3. バックアップするリソースを選択します。
4. [リソース] ページで、[スナップショット コピーにカスタム名形式を使用する] を選択し、スナップショット名に使用するカスタム名形式を入力します。

たとえば、*customtext_policy_hostname* または *resource_hostname* です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

5. [Application Settings] ページで、次の操作を実行します。

- 追加のバックアップ オプションを設定するには、[バックアップ] 矢印を選択します。

必要に応じて、整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for "Consistency Group Snapshot" operation to complete	スナップショット操作が完了するまでの待機時間を指定するには、「緊急」、または「中」、または「緩和」を選択します。[Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

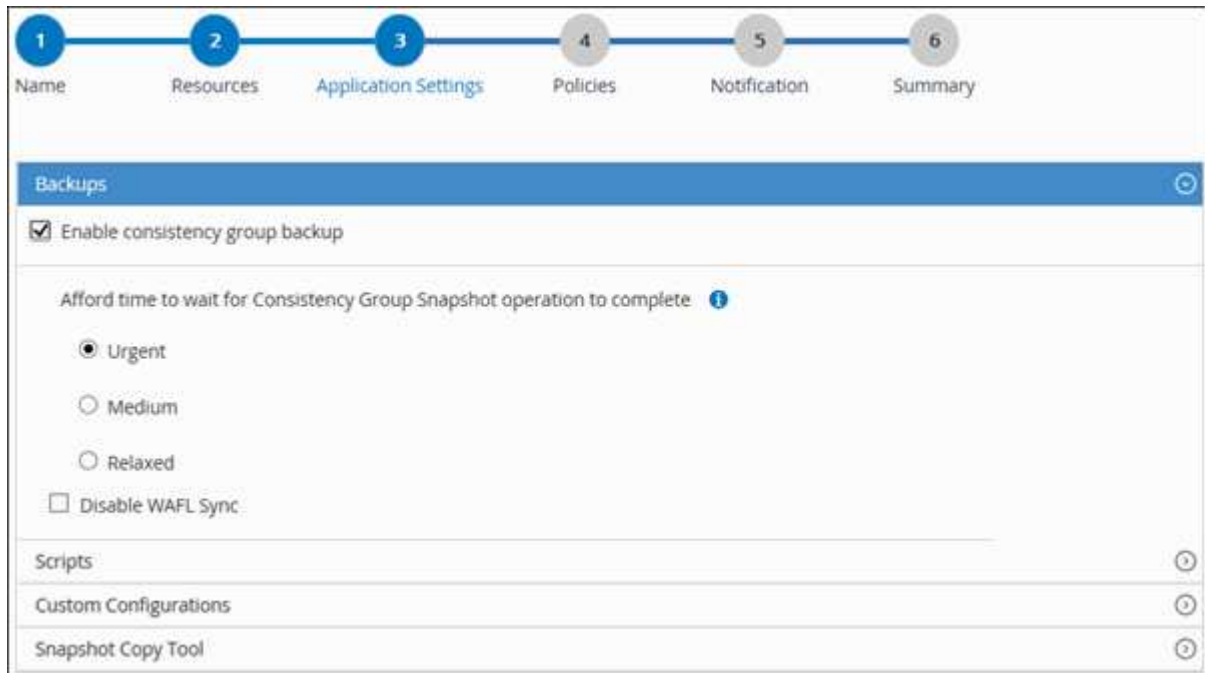
- *スクリプト*矢印を選択して、静止、スナップショット、および静止解除操作の事前および事後コマンドを実行します。

バックアップ処理を終了する前のプリコマンドも実行できます。プリスクリプトとポストスクリプトはSnapCenter Serverで実行されます。

- カスタム構成矢印を選択し、このリソースを使用するすべてのジョブに必要なカスタム値のペアを入力します。
- スナップショット コピー ツール 矢印を選択して、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでストレージ レベルのSnapshotを作成する	• ファイル システムの整合性のないSnapCenter * を選択します。

あなたが望むなら...	操作
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する	ファイル システムの一貫性を備えたSnapCenter * を選択します。
Snapshotを作成するためのコマンドを入力する	*その他*を選択し、スナップショットを作成するコマンドを入力します。



6. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます 。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b.  を選択
スケジュールを構成するポリシーの [スケジュールの構成] 列で、
- c. ポリシー *policy_name* のスケジュールの追加 ダイアログ ボックスでスケジュールを構成し、[OK] を選択します。

policy_name は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

7. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。

す。SMTP は、設定 > グローバル設定 でも設定する必要があります。

8. 概要を確認し、[完了] を選択します。

リソースのトポロジ ページが表示されます。

9. *今すぐバックアップ*を選択します。

10. [Backup]ページで次の手順を実行します。

- a. リソースに複数のポリシーを適用した場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*を選択します。

11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

- MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

詳細については、以下を参照してください。 ["MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"](#)

- VMDK上のアプリケーション データをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープ サイズが不足していると、バックアップが失敗することがあります。

Java ヒープ サイズを増やすには、スクリプト ファイル `/opt/netapp/init_scripts/scvservice` を見つけます。このスクリプトでは、`do_start method` コマンドによってSnapCenter VMware プラグイン サービスが開始されます。このコマンドを次のように更新します: `Java -jar -Xmx8192M -Xms4096M`

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmResourcesコマンドレットを使用して、手動リソースを追加します。

次の例は、PostgreSQLインスタンスを追加する方法を示しています。

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL
-ResourceType Instance -ResourceName postgresqlinst1
-StorageFootPrint
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_
data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Add-SmPolicyコマンドレットを使用して、バックアップ ポリシーを作成します。
4. リソースを保護するか、Add-SmResourceGroupコマンドレットを使用してSnapCenterに新しいリソース グループを追加します。
5. New-SmBackupコマンドレットを使用して、新しいバックアップ ジョブを開始します。

この例は、リソース グループをバックアップする方法を示しています。

```
C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-
clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
-Policy postgresql_policy1
```

この例では、保護されたリソースをバックアップしています。

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
-Policy postgresql_policy2
```

6. Get-smJobSummaryReportコマンドレットを使用して、ジョブのステータス（実行中、完了、失敗）を確認します。

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Get-SmBackupReportコマンドレットを使用して、リストアやクローニングの処理を実行するバックアップIDとバックアップ名など、バックアップ ジョブの詳細を監視します。

```

PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :

```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

リソース グループのバックアップ

リソース グループは、ホスト上のリソースの集まりです。リソース グループのバックアップ処理は、リソース グループに定義されているすべてのリソースを対象に実行されます。

開始する前に

- ポリシーを適用したリソース グループを作成しておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。

タスク概要

リソース グループは、[Resources]ページからオンデマンドでバックアップできます。リソース グループにポ

リシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが行われます。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。

リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、 をクリックして、タグを選択します。次に選択できます  フィルター パネルを閉じます。

3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] を選択します。
4. [Backup] ページで次の手順を実行します。
 - a. リソース グループに複数のポリシーを関連付けた場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*を選択します。

5. モニター > ジョブ を選択して、操作の進行状況を監視します。

PostgreSQLのバックアップ処理の監視

SnapCenterの[Jobs]ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*ジョブ*をクリックします。
3. [Jobs]ページで、次の手順を実行します。

- a. をクリックして、 リストの内容をバックアップ処理だけに絞り込みます。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*バックアップ*を選択します。
 - d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. バックアップ ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスは  ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[Activity]ペインでのPostgreSQLクラスタのデータ保護処理の監視

[Activity]ペインには、最後に実行された5つの処理が表示されます。また[Activity]ペインには、処理が開始された日次と処理のステータスが表示されます。

[Activity]ペインには、バックアップ、リストア、クローニング、スケジュールされたバックアップの各処理に関する情報が表示されます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. クリック  アクティビティ ペインで、最新の 5 つの操作を表示します。

いずれかの操作をクリックすると、*ジョブの詳細*ページに操作の詳細が表示されます。

PostgreSQLのバックアップ処理のキャンセル

キューに登録されているバックアップ処理はキャンセルできます。

必要なもの

- 処理をキャンセルするには、SnapCenter管理者かジョブ所有者としてログインする必要があります。
- バックアップ操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のバックアップ処理はキャンセルできません。
- バックアップ処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。
- キャンセルできない操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたバックアップ操作をキャンセルできます。

手順

1. 次のいずれかを実行します。

方法	アクション
[Monitor]ページ	a. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 b. 操作を選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	a. バックアップ操作を開始したら、*をクリックします。 * アクティビティ ペインで、最新の5つの操作を表示します。 b. 処理を選択します。 c. ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

処理がキャンセルされ、リソースは処理前の状態に戻ります。

[Topology]ページでのPostgreSQLのバックアップとクローンの表示

リソースのバックアップまたはクローニングを準備する際に、プライマリ ストレージとセカンダリ ストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。

タスク概要

プライマリ ストレージまたはセカンダリ ストレージ（ミラー コピーまたはバックアップ コピー）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

-  プライマリ ストレージで使用可能なバックアップとクローンの数を表示します。
-  SnapMirrorテクノロジーを使用してセカンダリ ストレージにミラーリングされているバックアップとクローンの数を表示します。
-  SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップとクローンの数を表示します。



表示されるバックアップの数には、セカンダリ ストレージから削除されたバックアップも含まれます。たとえば、バックアップを4個保持するポリシーを使用してバックアップを6個作成した場合、バックアップの数は6個と表示されます。



mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップの数にはバージョンに依存しないバックアップは含まれません。

[Topology]ページでは、選択したリソースまたはリソースグループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を参照し、対象を選択してデータ保護処理を実行できます。

手順

1. 左側のナビゲーションペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リソースの詳細ビューまたはリソースグループの詳細ビューで、リソースを選択します。

リソースが保護されている場合は、選択したリソースのトポロジページが表示されます。

4. *概要カード*を確認して、プライマリストレージとセカンダリストレージで使用可能なバックアップとクローンの数の概要を確認します。

概要カードセクションには、スナップショットコピーベースのバックアップとクローンの合計数が表示されます。

更新ボタンをクリックすると、ストレージのクエリが開始され、正確な数が表示されます。

SnapLock対応バックアップが取得された場合、[更新] ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでも、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限はONTAPから取得されます。

オンデマンドバックアップ後、[更新] ボタンをクリックすると、バックアップまたはクローンの詳細が更新されます。

5. 「コピーの管理」ビューで、プライマリストレージまたはセカンダリストレージからバックアップまたはクローンをクリックして、バックアップまたはクローンの詳細を表示します。

バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、削除の各処理を実行します。



セカンダリストレージ上のバックアップは、名前変更または削除できません。

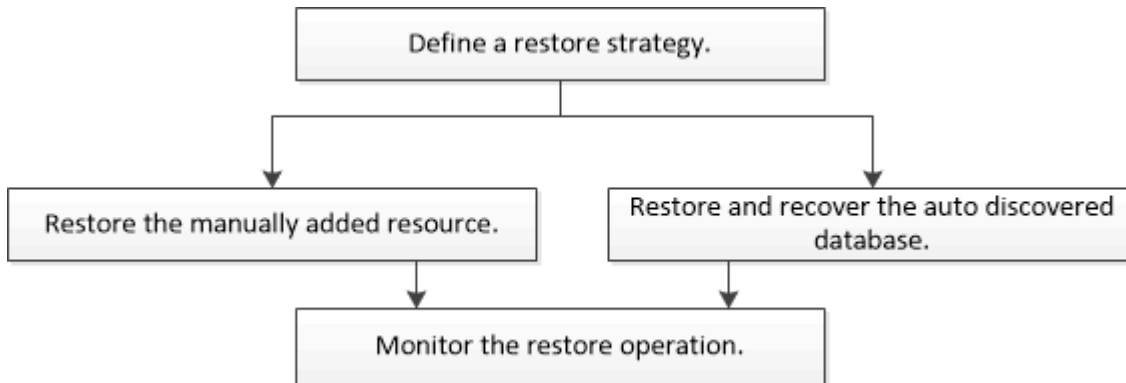
7. クローンを削除する場合は、表でクローンを選択し、 をクリックします。
8. クローンを分割する場合は、テーブルからクローンを選択し、。

PostgreSQLのリストア

リストアのワークフロー

リストアとリカバリのワークフローには、計画、リストア処理の実行、および処理の監視が含まれます。

次のワークフローは、リストア処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトでを使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

手動で追加されたリソース バックアップのリストアとリカバリ

SnapCenterを使用して1つまたは複数のバックアップからデータをリストアおよびリカバリすることができます。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- リストアするリソースまたはリソース グループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- リストア前、リストア後、マウント、アンマウントの各コマンドを実行する場合は、プラグイン ホストで次のパスから使用可能なコマンド リストにコマンドが存在するかどうかを確認する必要があります。
 - Windows ホスト上のデフォルトの場所: `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux ホスト上のデフォルトの場所: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホスト、関連するリソース グループとポリシー、およびステータスとともに表示されます。



リストアの実行時は、バックアップがリストア グループに対するものであっても、リストア対象のリソースを個別に選択する必要があります。

リソースが保護されていない場合は、「全体ステータス」列に「保護されていません」と表示されます。この状態になるのは、リソースが保護されていない場合とリソースが別のユーザによってバックアップされている場合です。

3. リソースを選択するか、リソース グループを選択してそのグループ内のリソースを選択します。

リソースのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージ システムから [バックアップ] を選択します。
5. プライマリバックアップテーブルで、復元するバックアップを選択し、*をクリックします。  *

Primary Backup(s)	
search 	  
Backup Name	End Date
rg1_scspr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. 復元範囲ページで、*完全なリソース*を選択します。
 - a. *完全なリソース*を選択すると、PostgreSQL クラスターのすべての構成済みデータ ボリュームが復元されます。

リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeのリストア用のSnapshotが選択されたあとに作成されたSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。

複数のLUNを選択できます。



すべて を選択すると、ボリューム、qtree、または LUN 上のすべてのファイルが復元されます。

7. [Pre ops] ページで、リストア ジョブの実行前に実行するリストア前の処理とアンマウントのコマン

ドを入力します。

自動検出されたリソースにはアンマウント コマンドを使用できません。

8. [Post ops]ページで、リストア ジョブの実行後に実行するマウントとリストア後の処理のコマンドを入力します。

自動検出されたリソースにはマウント コマンドを使用できません。

9. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP は、[設定] > [グローバル設定] ページでも設定する必要があります。

10. 概要を確認し、[完了] をクリックします。

11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよびGet-SmBackupReportコマンドレットを使用して、リストアする1つまたは複数のバックアップに関する情報を取得します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackupコマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

自動検出されたクラスタ バックアップのリストアとリカバリ

SnapCenterを使用して1つまたは複数のバックアップからデータをリストアおよびリカバリすることができます。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- リストアするリソースまたはリソース グループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- リストア前、リストア後、マウント、アンマウントの各コマンドを実行する場合は、プラグイン ホストで次のパスから使用可能なコマンド リストにコマンドが存在するかどうかを確認する必要があります。

- Windows ホスト上のデフォルトの場所: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux ホスト上のデフォルトの場所: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- ファイルベースのバックアップのコピーをSnapCenterからリストアすることはできません。
- 自動検出されたリソースについては、SFSRでリストアがサポートされます。
- 自動リカバリはサポートされていません。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホスト、関連するリソース グループとポリシー、およびステータスとともに表示されます。



リストアの実行時は、バックアップがリストア グループに対するものであっても、リストア対象のリソースを個別に選択する必要があります。

リソースが保護されていない場合は、「全体ステータス」列に「保護されていません」と表示されます。この状態になるのは、リソースが保護されていない場合とリソースが別のユーザによってバックアップされている場合です。

3. リソースを選択するか、リソース グループを選択してそのグループ内のリソースを選択します。

リソースのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボールド化された) ストレージシステムから [バックアップ] を選択します。
5. プライマリバックアップテーブルで、復元するバックアップを選択し、*をクリックします。



6. 「復元範囲」 ページで、「完全なリソース」を選択して、PostgreSQL クラスターの構成済みデータ ボリュームを復元します。

7. [Recovery scope]ページで、次のいずれかのオプションを選択します。

状況	操作
現在の時刻にできる限り近い時点にリカバリする場合	*最新の状態に回復*を選択します。単一コンテナ リソースの場合は、ログおよびカタログ バックアップの場所を1つ以上指定します。
指定した時点にリカバリする場合	*特定の時点に回復*を選択します。 a. 日時を入力します。日時を入力します。たとえば、PostgreSQL Linuxホストがカリフォルニア州サニーベールにあり、ノースカロライナ州ローリーにいるユーザがログをSnapCenterにリカバリしようとしているとします。 ユーザがカリフォルニア州サニーベールの午前5時にリカバリを実行したい場合、ユーザはブラウザのタイムゾーンをPostgreSQL Linuxホストのタイムゾーン（GMT-07:00）に設定し、日付と時刻を午前5時に指定する必要があります。
リカバリが不要である場合	*回復なし*を選択します。



手動で追加したPostgreSQLリソースはリカバリできません。



PostgreSQL 用のSnapCenterプラグインは、手動でのリカバリを支援するために、`/<OS_temp_folder>/postgresql_sc_recovery<Restore_JobId>/_` フォルダに `backup_label` と `tablespace_map` を作成します。

1. [Pre ops]ページで、リストア ジョブの実行前に実行するリストア前の処理とアンマウントのコマンドを入力します。

自動検出されたリソースにはアンマウント コマンドを使用できません。

2. [Post ops]ページで、リストア ジョブの実行後に実行するマウントとリストア後の処理のコマンドを入力します。

自動検出されたリソースにはマウント コマンドを使用できません。

3. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP は、[設定] > [グローバル設定] ページでも設定する必要があります。

4. 概要を確認し、[完了] をクリックします。
5. モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレットを使用したリソースのリストア

リソースのバックアップをリストアするときは、SnapCenter Serverとの接続セッションを開始し、バックアップをリストしてバックアップの情報を取得し、バックアップをリストアします。

PowerShellコマンドレットを実行できるように環境を準備しておく必要があります。

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよびGet-SmBackupReportコマンドレットを使用して、リストアする1つまたは複数のバックアップに関する情報を取得します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。


```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. Restore-SmBackupコマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

PostgreSQLのリストア処理の監視

[Job]ページを使用して、SnapCenterの各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中

-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター* ページで、*ジョブ* をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  でリストをフィルタリングし、リストア処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ* ドロップダウンリストから*復元*を選択します。
 - d. *ステータス* ドロップダウンリストから、復元ステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. 復元ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細* ページで、*ログの表示* をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

PostgreSQL リソースのバックアップのクローニング

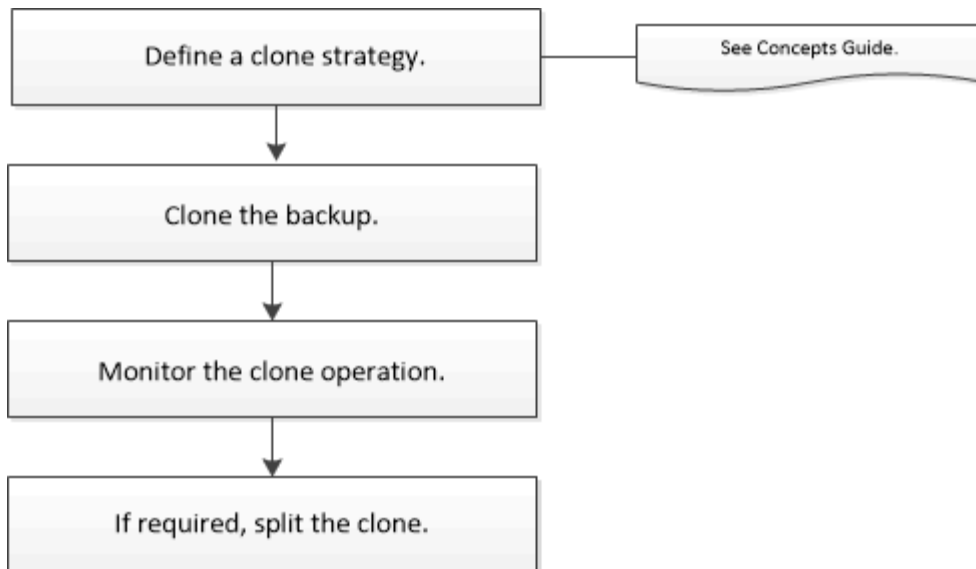
クローニングのワークフロー

クローニング ワークフローには、クローニング処理の実行と処理の監視が含まれます。

タスク概要

- ソース PostgreSQL サーバでクローニング処理を実行できます。
- リソースのバックアップをクローニングする理由には次のものがあります。
 - アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のリソースの構造およびコンテナツを使用してテストするため
 - データの抽出と操作を行うツールで、データ ウェアハウスにデータを取り込むため
 - 誤って削除または変更されたデータをリカバリするため

次のワークフローは、クローニング処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

PostgreSQLのバックアップのクローニング

SnapCenterを使用してバックアップをクローニングすることができます。クローニングはプライマリとセカンダリのどちらのバックアップからも実行できます。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- ボリュームをホストするアグリゲートがStorage Virtual Machine (SVM) の割り当て済みアグリゲート リストに含まれていることを確認します。
- クローニング前またはクローニング後のコマンドについては、プラグイン ホストの次のパスで使用できるコマンド リストにコマンドが存在するかどうかを確認する必要があります。
 - Windows ホスト上のデフォルトの場所: `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux ホスト上のデフォルトの場所: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- FlexCloneボリューム分割操作の詳細については、以下を参照してください。 <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["親ボリュームからのFlexCloneボリュームのスプリット"]。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホスト、関連するリソース グループとポリシー、ステータスなどの情報とともに表示されます。

3. リソースまたはリソース グループを選択します。

リソース グループを選択した場合はリソースを選択する必要があります。

リソースまたはリソース グループのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージ システムから [バックアップ] を選択します。
5. 表からデータバックアップを選択し、クリックします。 。
6. [Location] ページで、次の操作を実行します。

フィールド	操作
Clone server	クローンをどのホスト上に作成するかを選択します。
Target Port	既存のバックアップからクローニングするPostgreSQLのターゲット ポートを入力します。
NFS Export IP Address	クローン ボリュームをエクスポートするホスト名またはIPアドレスを入力します。 これは、NFSストレージ タイプのリソースにのみ該当します。
Capacity Pool Max. Throughput (MiB/s)	容量プールの最大スループットを入力します。 これは、ANFストレージ タイプのリソースにのみ該当します。

7. [Scripts] ページで、次の手順を実行します。



スクリプトはプラグイン ホストで実行されます。

- a. クローニング処理の前後に実行するプリコマンドやポストコマンドを入力します。

- クローン前のコマンド: 同じ名前の既存のクラスターを削除する
- クローン後のコマンド: クラスターを検証するか、クラスターを起動します。

b. ホストにファイルシステムをマウントするには、mountコマンドを入力します。

Linuxマシンのボリュームまたはqtreeに対するmountコマンド：

NFSの例: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。

9. 概要を確認し、[完了] をクリックします。
10. モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットを使用して、クローニング処理を実行するバックアップを取得します。

この例では、クローニングできるバックアップが2つあります。

```
C:\PS> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
1	Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM	

3. 既存のバックアップからクローニング処理を開始し、クローニングされたボリュームをエクスポートするNFSエクスポートのIPアドレスを指定します。

この例では、NFSExportIPsのアドレスを10.32.212.14と指定してバックアップをクローニングしています。

PostgreSQLクラスタの場合：

```
PS C:\> New-SmClone -AppPluginCode PostgreSQL -BackupName "
scpostgresql01_ openenglab_netapp_com_PostgreSQL_postgres_5432_06-
26-2024_00_33_41_1570" -Resources @{"Host"="
10.32.212.13";"Uid"="postgres_5432"} -port 2345 -CloneToHost
10.32.212.14
```



NFSExportIPsを指定しない場合、デフォルトでクローン ターゲット ホストにエクスポートされます。

4. Get-SmCloneReportコマンドレットを使用してクローニング ジョブの詳細を表示し、バックアップが正常にクローニングされたことを確認します。

クローンID、開始日時、終了日時などの詳細を確認できます。

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration              : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName            : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName      : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName             : Draper__clone__08-03-2015_14.43.53
SourceResources       : {Don, Betty, Bobby, Sally}
ClonedResources       : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError            :
```

PostgreSQLのクローン処理の監視

SnapCenterのクローニング処理の進捗状況を、[Jobs]ページで監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  てリストをフィルタリングし、クローニング処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*クローン*を選択します。
 - d. *ステータス*ドロップダウンリストからクローンのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. クローンジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. ジョブの詳細ページで、*ログの表示*をクリックします。

クローンのスプリット

SnapCenterを使用して、クローン リソースを親リソースからスプリットできます。スプリットされたクローンは親リソースから独立します。

タスク概要

- 中間クローンではクローン スプリット処理を実行できません。

たとえば、データベース バックアップからクローン1を作成したあとで、クローン1のバックアップを作成し、そのバックアップ（クローン2）をクローニングできます。クローン2を作成すると、クローン1は中間クローンになり、クローン1ではクローン スプリット処理を実行できなくなります。ただし、クローン2に対してはクローン スプリット処理を実行できます。

クローン2をスプリットすると、クローン1は中間クローンではなくなるため、クローン1に対してクローン スプリット処理を実行できるようになります。

- クローンをスプリットすると、そのクローンのバックアップ コピーとクローン ジョブが削除されます。
- FlexCloneボリューム分割操作の詳細については、以下を参照してください。 ["親ボリュームからFlexCloneボリュームのスプリット"](#)。
- ストレージ システム上のボリュームまたはアグリゲートがオンラインであることを確認します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. *リソース* ページで、表示リストから適切なオプションを選択します。

オプション	説明
データベース アプリケーションの場合	表示リストから*データベース*を選択します。
ファイルシステムの場合	表示リストから*パス*を選択します。

3. リストから適切なリソースを選択します。

リソースのトポロジ ページが表示されます。

4. *コピーの管理*ビューから、クローンされたリソース（データベースやLUNなど）を選択し、*をクリックします。  *。
5. 分割するクローンの推定サイズとアグリゲート上で必要な空き容量を確認し、[開始] をクリックします。
6. モニター > ジョブ をクリックして、操作の進行状況を監視します。

SMCoreサービスが再起動されると、クローン スプリット処理は応答を停止します。Stop-SmJobコマンドレットを実行してクローン スプリット処理を停止してから、クローン スプリット処理を再試行してください。

クローンが分割されているかどうかを確認するためのポーリング時間を長くしたり短くしたりする場合は、*SMCoreServiceHost.exe.config* ファイルの *CloneSplitStatusCheckPollTime* パラメータの値を変更して、SMCore がクローン分割操作のステータスをポーリングする時間間隔を設定できます。値はミリ秒単位で、デフォルト値は5分です。

例えば：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

バックアップ、リストア、または別のクローン スプリットが実行中の場合、クローン スプリットの開始処理は失敗します。クローン スプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

["アグリゲートが存在しないためにSnapCenterのクローニングや検証が失敗する"](#)

SnapCenterアップグレード後のPostgreSQLクラスタのクローンの削除またはスプリット

SnapCenter 4.3にアップグレードすると、クローンは表示されなくなります。クローンを作成したリソースの[Topology]ページで、クローンの削除やスプリットを実行できます。

タスク概要

非表示のクローンのストレージ フットプリントを見つける場合は、次のコマンドを実行します。 `Get-SmClone -ListStorageFootprint`

手順

1. `remove-smbackup` コマンドレットを使用して、クローニングされたリソースのバックアップを削除します。
2. `remove-smresourcegroup` コマンドレットを使用して、クローニングされたリソースのリソース グループを削除します。
3. `remove-smprotectresource` コマンドレットを使用して、クローニングされたリソースの保護を解除します。
4. [Resources] ページで親リソースを選択します。

リソースのトポロジ ページが表示されます。

5. [Manage Copies] ビューで、プライマリまたはセカンダリ（ミラー先またはレプリケート先）ストレージシステムからクローンを選択します。
6. クローンを選択し、クリックします  クローンを削除するには、または  クローンを分割します。
7. [OK] をクリックします。

MySQLの保護

SnapCenter Plug-in for MySQL

SnapCenter Plug-in for MySQLの概要

SnapCenter Plug-in for MySQL Databaseは、MySQLデータベースに対してアプリケーション対応のデータ保護管理を可能にする、NetApp SnapCenterソフトウェアのホスト側コンポーネントです。Plug-in for MySQL Databaseは、SnapCenter環境でのMySQLデータベースのバックアップ、リストア、およびクローニングを自動化します。

SnapCenterは、単一インスタンスのMySQLセットアップをサポートしています。Plug-in for MySQL Databaseは、WindowsとLinuxのどちらの環境でも使用できます。Windows環境では、MySQLは手動リソースとしてサポートされます。

Plug-in for MySQL Databaseがインストールされている場合は、SnapCenterとNetApp SnapMirrorテクノロジーを使用して、バックアップセットのミラーコピーを別のボリュームに作成できます。また、このプラグインをNetApp SnapVaultテクノロジーとともに使用して、標準への準拠を目的としたディスクツーディスクバックアップレプリケーションを実行することもできます。

SnapCenter Plug-in for MySQLは、ONTAPおよびAzure NetApp FilesストレージレイアウトでNFSとSANをサポートします。

VMDK、vVol、RDM 仮想ストレージレイアウトがサポートされています。

シンボリックリンクはサポートされません。

SnapCenter Plug-in for MySQLの機能

Plug-in for MySQL Databaseをインストールした環境では、SnapCenterを使用してMySQLインスタンスをバックアップ、リストア、クローニングできます。これらの処理をサポートするタスクも実行できます。

- インスタンスを追加します。
- バックアップを作成します。
- バックアップからリストアします。
- バックアップをクローニングします。
- バックアップ処理のスケジュールを設定します。
- バックアップ、リストア、クローニングの各処理を監視します。
- バックアップ、リストア、クローニングの各処理のレポートを表示します。

SnapCenter Plug-in for MySQLの特長

SnapCenterは、プラグインアプリケーションと統合されるほか、ストレージシステム上でNetAppの数々のテクノロジーと統合されます。Plug-in for MySQL Databaseの操作に

は、SnapCenterのグラフィカル ユーザ インターフェイスを使用します。

- 統合されたグラフィカルユーザーインターフェース

SnapCenterのインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。どのプラグインでも、SnapCenterのインターフェイスから、バックアップ、リストア、クローニングの各処理を一貫した方法で実行できるほか、ダッシュボード ビューで概要を把握したり、ロールベース アクセス制御（RBAC）を設定したり、ジョブを監視したりすることができます。

- 自動化された中央管理

バックアップ処理のスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理を実行したりできます。SnapCenterからのEメール アラートの送信を設定して、環境をプロアクティブに監視することもできます。

- 無停止の**NetApp**スナップショット コピー テクノロジー

SnapCenterでは、Plug-in for MySQL DatabaseでNetApp Snapshotテクノロジーを使用してリソースがバックアップされます。

Plug-in for MySQLを使用すると、次のメリットもあります。

- バックアップ、リストア、およびクローニングのワークフローがサポートされます。
- セキュリティがRBACでサポートされ、ロール委譲が一元化されます。

クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルのアクセス権を付与することもできます。

- NetApp FlexCloneテクノロジーを使用して、テストまたはデータ抽出に使用するリソースのコピー（スペース効率に優れたポイントインタイム コピー）を作成できます。

クローンを作成するストレージ システムにFlexCloneライセンスが必要です。

- バックアップの作成でONTAPの整合グループ（CG）のSnapshot機能がサポートされます。
- 複数のリソース ホストで同時に複数のバックアップを実行できます。

1回の処理で、1つのホストの複数のリソースが同じボリュームを共有する場合に複数のSnapshotが統合されます。

- 外部コマンドを使用してSnapshotを作成できます。
- XFSファイルシステム上のLinux LVMがサポートされます。

SnapCenter Plug-in for MySQLでサポートされるストレージ タイプ

SnapCenterは、物理マシンと仮想マシン（VM）の両方でさまざまなストレージ タイプをサポートしています。SnapCenter Plug-in for MySQLをインストールする前に、ストレージ タイプがサポートされているかどうかを確認する必要があります。

マシン	ストレージ タイプ
物理サーバ	• FC接続LUN • iSCSI接続LUN • NFS接続ボリューム
VMware ESXi	• FCまたはiSCSI HBAで接続されたRDM LUNホスト バス アダプタ (HBA) のスキャン は、SnapCenterがホストに存在するすべてのホスト バス アダプタをスキャンするため、完了までに時間がかかることがあります。 <i>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</i> にある LinuxConfig.pm ファイルを編集し て、SCSI_HOSTS_OPTIMIZED_RESCAN パラメータの値を 1 に設定し、HBA_DRIVER_NAMES にリストされているHBA のみを再スキャンすることができます。 • iSCSIイニシエータでゲスト システムに直接接続されたiSCSI LUN • NFSデータストア上のVMDK • VMFS上にVMDKが作成されました • ゲスト システムに直接接続されたNFSボリューム • NFSとSANの両方に存在するvVolデータストア vVolデータストアは、ONTAP Tools for VMware vSphereでのみプロビジョニングできます。

MySQLプラグインに必要な最小ONTAP権限

必要な最小ONTAP権限は、データ保護に使用するSnapCenterプラグインによって異なります。

- 全アクセス コマンド: ONTAP 9.12.1 以降に必要な最小限の権限
 - event generate-autosupport-log
 - job history show
 - job stop
 - lun
 - lun create
 - lun create

- lun create
- lun delete
- lun igroup add
- lun igroup create
- lun igroup delete
- lun igroup rename
- lun igroup rename
- lun igroup show
- lun mapping add-reporting-nodes
- lun mapping create
- lun mapping delete
- lun mapping remove-reporting-nodes
- lun mapping show
- lun modify
- lun move-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- lun resize
- lun serial
- lun show
- snapmirror policy add-rule
- snapmirror policy modify-rule
- snapmirror policy remove-rule
- snapmirror policy show
- snapmirror restore
- snapmirror show
- snapmirror show-history
- snapmirror update
- snapmirror update-ls-set
- snapmirror list-destinations
- version
- volume clone create
- volume clone show
- volume clone split start
- volume clone split stop
- volume create

- volume destroy
- volume file clone create
- volume file show-disk-usage
- volume offline
- volume online
- volume modify
- volume qtree create
- volume qtree delete
- volume qtree modify
- volume qtree show
- volume restrict
- volume show
- volume snapshot create
- volume snapshot delete
- volume snapshot modify
- volume snapshot modify-snaplock-expiry-time
- volume snapshot rename
- volume snapshot restore
- volume snapshot restore-file
- volume snapshot show
- volume unmount
- vservers cifs
- vservers cifs share create
- vservers cifs share delete
- vservers cifs shadowcopy show
- vservers cifs share show
- vservers cifs show
- vservers export-policy
- vservers export-policy create
- vservers export-policy delete
- vservers export-policy rule create
- vservers export-policy rule show
- vservers export-policy show
- vservers iscsi
- vservers iscsi connection show
- vservers show

- 読み取り専用コマンド: ONTAP 8.3.0以降に必要な最小限の権限

- ネットワークインターフェース
- network interface show
- SVM

MySQLでのSnapMirrorレプリケーションとSnapVaultレプリケーションのためのストレージシステムの準備

SnapCenterプラグインと一緒にONTAP SnapMirrorテクノロジーを使用すると、バックアップセットのミラー コピーを別のボリュームに作成できます。また、ONTAP SnapVaultを使用すれば、標準への準拠やその他のガバナンスを目的としたディスクツェーディスクのバックアップ レプリケーションを実行できます。これらのタスクを実行する前に、ソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenterは、Snapshot処理の完了後に、SnapMirrorとSnapVaultに対する更新を実行します。SnapMirror更新とSnapVault更新は、SnapCenterジョブの一部として実行されるため、ONTAPスケジュールを別途作成しないでください。



NetApp SnapManager製品からSnapCenterに移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリ ストレージ（ソース ボリューム）上のデータがセカンダリ ストレージ（デスティネーション ボリューム）にレプリケートされます。この関係を初期化すると、ソース ボリュームで参照されるデータ ブロックがデスティネーション ボリュームに転送されます。



SnapCenter は、SnapMirrorとSnapVaultボリューム間のカスケード関係をサポートしていません（* プライマリ * > ミラー > ボールト）。ファンアウト関係を使用する必要があります。

SnapCenterは、バージョンに依存しないSnapMirror関係の管理をサポートしています。バージョンに依存しないSnapMirror関係とその設定方法の詳細については、["ONTAPのドキュメント"](#)。

MySQLのバックアップ戦略

MySQLのバックアップ戦略の定義

バックアップ ジョブを作成する前にバックアップ戦略を定義しておく、リソースの正常なリストアやクローニングに必要なバックアップを作成するのに役立ちます。バックアップ戦略の大部分は、サービス レベル アグリーメント（SLA）、目標復旧時間（RTO）、および目標復旧時点（RPO）によって決まります。

タスク概要

SLAとは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。RTOは、サービスの停止からビジネス プロセスの復旧までに必要となる時間です。RPOは、障害発生後に通常処理を再開するためにバックアップ ストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA、RTO、およびRPOは、データ保護戦略に関与します。

手順

1. リソースをバックアップするタイミングを決定します。
2. 必要なバックアップ ジョブの数を決定します。
3. バックアップの命名方法を決定します。
4. Snapshotコピーベースのポリシーを作成してアプリケーションと整合性のあるデータベースのSnapshotをバックアップするかどうかを決定します。
5. レプリケーションのためにNetApp SnapMirrorテクノロジーを使用するか、または長期保持のためにNetApp SnapVaultテクノロジーを使用するかを決定します。
6. ソース ストレージ システムおよびSnapMirrorデスティネーションでのSnapshotの保持期間を確認します。
7. バックアップ処理の前後にコマンドを実行するかどうかを決定し、実行する場合はプリスクリプトまたはポストスクリプトを用意します。

Linuxホスト上のリソースの自動検出

リソースとは、SnapCenterで管理するLinuxホスト上のMySQLインスタンスです。SnapCenter Plug-in for MySQLプラグインをインストールすると、そのLinuxホスト上のMySQLインスタンスが自動的に検出されて[Resources]ページに表示されます。

サポートされるバックアップのタイプ

バックアップ タイプでは、作成するバックアップのタイプを指定します。SnapCenterでは、MySQLデータベースに対してSnapshotコピーベースのバックアップ タイプがサポートされます。

Snapshotコピーベースのバックアップ

Snapshotコピーベースのバックアップでは、NetApp Snapshotテクノロジーを利用して、MySQLデータベースが格納されたボリュームのオンラインの読み取り専用のコピーが作成されます。

SnapCenter Plug-in for MySQLでの整合グループSnapshotの使用方法

プラグインを使用して、リソース グループの整合グループSnapshotを作成することができます。整合グループとはボリュームのコンテナであり、複数のボリュームを格納して1つのエンティティとして管理できます。整合グループには複数のボリュームの同時に作成されたSnapshotが格納されるため、一連のボリュームのコピーの整合性が確保されます。

ストレージ コントローラが整合性を確保しながらSnapshotをグループ化するのを待機する時間も指定できます。利用可能な待機時間のオプションは、「緊急」、「中」、「緩和」です。また、整合グループSnapshotの処理でWrite Anywhere File Layout (WAFL) の同期を有効にするか無効にするかも選択できます。WAFLの同期を有効にすると、整合グループSnapshotのパフォーマンスが向上します。

SnapCenterによる不要なログ バックアップの削除の管理

SnapCenterは、ストレージ システム レベルおよびファイルシステム レベルで不要なデータバックアップの削除を管理します。

MySQLのバックアップスケジュールを決定する際の考慮事項

バックアップのスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率です。使用頻度の高いリソースは1時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは1日に1回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービス レベル アグリーメント（SLA）、目標復旧時点（RPO）などがあります。

バックアップ スケジュールには、次の2つの要素があります。

- バックアップ頻度（バックアップを実行する間隔）

バックアップ頻度は、ポリシー設定の一部であり、一部のプラグインではスケジュール タイプとも呼ばれます。たとえば、毎時、毎日、毎週、または毎月としてバックアップ頻度を設定できます。

- バックアップ スケジュール（バックアップが実行される日時）

バックアップ スケジュールは、リソースまたはリソース グループの設定の一部です。たとえば、週次バックアップのポリシーが設定されているリソースグループがある場合、毎週木曜日の午後10時にバックアップするようにスケジュールを設定できます。

MySQLに必要なバックアップ ジョブの数

必要なバックアップ ジョブの数を左右する要因としては、リソースのサイズ、使用中のボリュームの数、リソースの変更率、サービス レベル アグリーメント（SLA）などがあります。

Plug-in for MySQLデータベースのバックアップの命名規則

Snapshotのデフォルトの命名規則を使用するか、カスタマイズした命名規則を使用できます。デフォルトのバックアップ命名規則ではSnapshot名にタイムスタンプが追加されるので、コピーが作成されたタイミングを特定できます。

Snapshotでは、次のデフォルトの命名規則が使用されます。

`resourcegroupname_hostname_timestamp`

バックアップ リソース グループには、次の例のように論理的な名前を付ける必要があります。

```
dts1_mach1x88_03-12-2015_23.17.26
```

この例では、各構文要素に次の意味があります。

- *dts1* はリソース グループ名です。
- *mach1x88* はホスト名です。
- *03-12-2015_23.17.26* は日付とタイムスタンプです。

または、[スナップショット コピーにカスタム名形式を使用する] を選択して、リソースまたはリソース グループを保護しながらスナップショット名の形式を指定することもできます。たとえば、`customtext_resourcegroup_policy_hostname`や`resourcegroup_hostname`などの形式です。デフォルトでは、Snapshot名にタイムスタンプのサフィックスが追加されます。

MySQLのリストアとリカバリ戦略

MySQLリソースのリストアとリカバリの戦略の定義

データベースのリストアとリカバリを行う前に戦略を定義しておく、リストア処理とリカバリ処理を正常に実行できるようになります。



データベースの手動リカバリのみがサポートされます。

手順

1. 手動で追加したMySQLリソースでサポートされるリストア戦略を確認します。
2. 自動検出されたMySQLデータベースでサポートされるリストア戦略を確認します。
3. 実行するリカバリ処理のタイプを決定します。

手動で追加したMySQLリソースでサポートされるリストア戦略のタイプ

SnapCenterを使用してリストア処理を正常に実行するには、戦略を定義しておく必要があります。手動で追加したMySQLリソースには、2種類のリストア戦略があります。



手動で追加したMySQLリソースはリカバリできません。

リソース全体のリストア

- リソースのすべてのボリューム、qtree、およびLUNをリストア



リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeのリストア用のSnapshotが選択されたあとに作成されたSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。

自動検出されたMySQLでサポートされるリストア戦略のタイプ

SnapCenterを使用してリストア処理を正常に実行するには、戦略を定義しておく必要があります。

リソースの完全リストアは、自動検出されたMySQLデータベースに対してサポートされているリストア戦略です。この戦略では、リソースのすべてのボリューム、qtree、およびLUNがリストアされます。

自動検出されたMySQLのリストア処理のタイプ

SnapCenter Plug-in for MySQLでは、自動検出されたMySQLデータベースに対して、Single File SnapRestoreおよびConnect and Copyのリストア タイプがサポートされ

ます。

NFS環境でSingle File SnapRestoreを実行するシナリオは、次のとおりです。

- *完全なリソース*オプションのみを選択した場合
- 選択したバックアップがSnapMirrorまたはSnapVaultのセカンダリロケーションからのものであり、*完全なリソース*オプションが選択されている場合

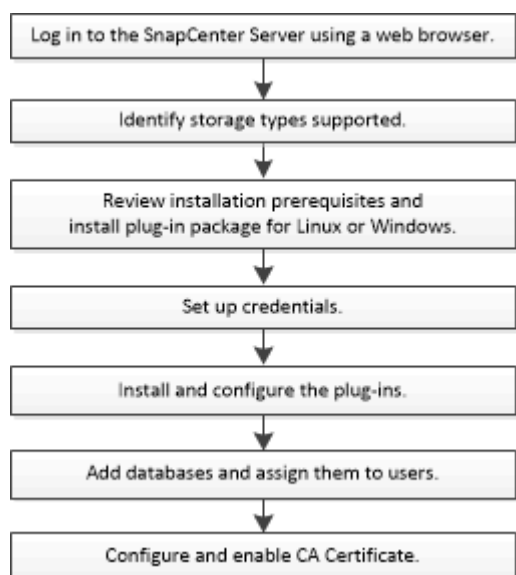
SAN環境でSingle File SnapRestoreを実行するシナリオは、次のとおりです。

- *完全なリソース*オプションのみを選択した場合
- バックアップがSnapMirrorまたはSnapVaultのセカンダリロケーションから選択され、*完全なリソース*オプションが選択されている場合

SnapCenter Plug-in for MySQLのインストール準備

SnapCenter Plug-in for MySQLのインストール ワークフロー

MySQLデータベースを保護する場合は、SnapCenter Plug-in for MySQLをインストールしてセットアップする必要があります。



ホストを追加して**SnapCenter Plug-in for MySQL**をインストールするための前提条件

ホストを追加してプラグイン パッケージをインストールする前に、すべての要件を満たしておく必要があります。SnapCenter Plug-in for MySQLは、WindowsとLinuxどちらの環境でも使用できます。

- Java 11をホストにインストールしておく必要があります。



IBM Java は Windows および Linux ホストではサポートされていません。

- Windows の場合、プラグイン クリエーター サービスは、"LocalSystem` Windows ユーザーを使用して実行する必要があります。これは、Plug-in for MySQL がドメイン管理者としてインストールされている場合のデフォルトの動作です。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。WindowsホストにMySQLプラグインをインストールすると、SnapCenter Plug-in for Microsoft Windowsもデフォルトで導入されます。
- SnapCenter Serverが、Plug-in for MySQLホストの8145ポートまたはカスタム ポートにアクセスできる必要があります。
- MySQL 5.7の場合は、MySQLの設定ファイル（my.cnfまたはmysql-server.cnf）にbinlogを指定する必要があります。

Windowsホスト

- ローカル管理者権限があり、リモート ホストに対してローカル ログインのアクセス許可があるドメイン ユーザが必要です。
- Plug-in for MySQLをWindowsホストにインストールすると、SnapCenter Plug-in for Microsoft Windowsが自動的にインストールされます。
- rootユーザまたはroot以外のユーザに対してパスワード ベースのSSH接続を有効にしておく必要があります。
- Java 11をWindowsホストにインストールしておく必要があります。

["すべてのオペレーティングシステム用のJAVAをダウンロード"](#)

["NetApp Interoperability Matrix Tool"](#)

Linuxホスト

- rootユーザまたはroot以外のユーザに対してパスワード ベースのSSH接続を有効にしておく必要があります。
- Java 11をLinuxホストにインストールしておく必要があります。

["すべてのオペレーティングシステム用のJAVAをダウンロード"](#)

["NetApp Interoperability Matrix Tool"](#)

- LinuxホストでMySQLデータベースを実行している場合は、Plug-in for MySQLのインストール時にSnapCenter Plug-in for UNIXが自動的にインストールされます。
- プラグインのインストールには、デフォルトのシェルとして **bash** を使用する必要があります。

補助コマンド

SnapCenterプラグイン for MySQL で補足コマンドを実行するには、そのコマンドを `allowed_commands.config` ファイルに含める必要があります。

- Windows ホスト上のデフォルトの場所: `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux ホスト上のデフォルトの場所: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`

プラグイン ホストで補足コマンドを許可するには、エディターで *allowed_commands.config* ファイルを開きます。各コマンドを別々の行に入力します。コマンドでは大文字と小文字は区別されません。完全修飾パス名を指定し、パス名にスペースが含まれている場合は引用符 (") で囲んでください。

例えば：

コマンド: mount コマンド: umount コマンド: "C:\Program Files\ NetApp\SnapCreator commands\sdcli.exe" コマンド: myscript.bat

allowed_commands.config ファイルが存在しない場合、コマンドまたはスクリプトの実行はブロックされ、ワークフローは次のエラーで失敗します。

"[/mnt/mount -a] の実行は許可されていません。Authorize by adding the command in the file %s on the plugin host."

コマンドまたはスクリプトが *allowed_commands.config* に存在しない場合、コマンドまたはスクリプトの実行はブロックされ、ワークフローは次のエラーで失敗します。

"[/mnt/mount -a] の実行は許可されていません。Authorize by adding the command in the file %s on the plugin host."



すべてのコマンドを許可するには、ワイルドカード エントリ (*) を使用しないでください。

Linuxホストのroot以外のユーザへのsudo権限の設定

SnapCenter、非ルート ユーザーが Linux 用のSnapCenterプラグイン パッケージをインストールし、プラグイン プロセスを開始できます。プラグイン プロセスは有効なroot以外のユーザとして実行されます。いくつかのパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

必要なもの

- sudoバージョン1.8.7以降
- umask が 0027 の場合、java フォルダーとその中のすべてのファイルに 555 の権限があることを確認します。そうしないと、プラグインのインストールが失敗する可能性があります。
- root以外のユーザについては、root以外のユーザの名前とユーザのグループが同じであることを確認してください。
- */etc/ssh/sshd_config* ファイルを編集して、メッセージ認証コード アルゴリズム (MAC hmac-sha2-256 および MAC hmac-sha2-512) を設定します。

この構成ファイルを更新したら、sshdサービスを再起動します。

例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

このタスクについて

次のパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /custom_location/NetApp/snapcenter/spl/bin/spl

手順

1. SnapCenter Plug-ins Package for LinuxをインストールするLinuxホストにログインします。
2. visudo Linuxユーティリティを使用して、/etc/sudoersファイルに次の行を追加します。

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```



RAC をセットアップしている場合は、他の許可されたコマンドとともに、`/etc/sudoers` ファイルに次の行を追加する必要があります: `'/<crs_home>/bin/olsnodes'`

`crs_home` の値は、`/etc/oracle/olr.loc` ファイルから取得できます。

`LINUX_USER` は、作成した非 root ユーザーの名前です。

`checksum_value` は、次の場所にある `sc_unix_plugins_checksum.txt` ファイルから取得できます。

- `_C:\ProgramData\NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _` (SnapCenter Server が Windows ホストにインストールされている場合)。
- `_/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _` SnapCenter Server が Linux ホストにインストールされている場合。



この例は、独自のデータを作成する際の参照としてのみ使用してください。

SnapCenter Plug-ins Package for Windowsをインストールするホストの要件

SnapCenter Plug-ins Package for Windowsをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	Microsoft Windows サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool" 。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	5 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。

項目	要件
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell Core 7.4.2 サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool"。

SnapCenter Plug-ins Package for Linuxをインストールするホストの要件

SnapCenter Plug-ins Package for Linuxをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	• Red Hat Enterprise Linux • SUSE Linux Enterprise Server (SLES) サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool"。
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	2 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	Java 11 Oracle JavaおよびOpenJDK Javaを最新バージョンにアップグレードした場合は、/var/opt/snapcenter/spl/etc/spl.propertiesにあるJAVA_HOMEオプションが正しいJavaバージョンと正しいパスに設定されていることを確認する必要があります。 サポートされているバージョンに関する最新情報については、 "NetApp Interoperability Matrix Tool"。

SnapCenter Plug-in for MySQLのクレデンシャルの設定

SnapCenterは、クレデンシャルを使用してSnapCenterの処理を実行するユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、データベースやWindowsファイルシステムでのデータ保護処理に使用するクレデンシャルをそれぞれ作成する必要があります。

タスク概要

- Linuxホスト

Linuxホストにプラグインをインストールするには、クレデンシャルを設定する必要があります。

このクレデンシャルは、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo権限があるroot以外のユーザに対して設定します。

ベスト プラクティス: ホストをデプロイしてプラグインをインストールした後も Linux の認証情報を作成できますが、ベスト プラクティスとしては、SVM を追加した後、ホストをデプロイしてプラグインをインストールする前に認証情報を作成します。

- Windowsホスト

プラグインのインストール前にWindowsクレデンシャルを設定する必要があります。

このクレデンシャルには、管理者権限（リモート ホストに対する管理者権限を含む）を設定する必要があります。

個々のリソース グループのクレデンシャルを設定する場合で、ユーザ名に完全なadmin権限が割り当てられていない場合は、少なくともリソース グループとバックアップの権限を割り当てる必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[資格情報]をクリックします。
3. *新規*をクリックします。
4. [Credential]ページで、クレデンシャルの設定に必要な情報を指定します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。

フィールド	操作
ユーザ名	認証に使用するユーザ名とパスワードを入力します。 - ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者またはSnapCenterプラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。ユーザ名フィールドの有効な形式は次のとおりです。 ◦ <i>NetBIOS</i>\ユーザー名 ◦ ドメイン<i>FQDN</i>\ユーザー名 - ローカル管理者（ワークグループの場合のみ） ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。ユーザー名フィールドの有効な形式は次のとおりです: <i>UserName</i> パスワードには二重引用符 (") やバッククォート (') を使用しないでください。未満記号 (<) と感嘆符 (!) を組み合わせて使用したりしないでください。たとえば、lessthan<!10、lessthan10<!、バックティック`12 などです。
パスワード	認証に使用するパスワードを入力します。
Authentication Mode	使用する認証モードを選択します。
Use sudo privileges	非 root ユーザーの資格情報を作成する場合は、[sudo 権限を使用する] チェックボックスをオンにします。  Linuxユーザのみに該当します。

5. [OK]をクリックします。

クレデンシャルの設定が完了したら、必要に応じて[User and Access]ページでユーザやユーザ グループにクレデンシャルを割り当てることができます。

SnapCenter Plug-in for MySQLのインストール

ホストの追加とリモート ホストへのプラグイン パッケージのインストール

SnapCenterの[Add Host]ページを使用してホストを追加し、プラグイン パッケージをインストールする必要があります。プラグインは、自動的にリモート ホストにインストールされます。ホストの追加とプラグイン パッケージのインストールは、ホストごとに実行できます。

開始する前に

- SnapCenter Serverホストのオペレーティング システムがWindows 2019で、プラグイン ホストのオペレーティング システムがWindows 2022の場合は、次の手順を実行する必要があります。
 - Windows Server 2019（OSビルド17763.5936）以降にアップグレードする
 - Windows Server 2022（OSビルド20348.2402）以降にアップグレードする
- この処理は、SnapCenter Adminロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。
- メッセージ キュー サービスが実行中であることを確認する必要があります。
- ホストの管理については、管理に関するドキュメントを参照してください。

タスク概要

- SnapCenter Serverをプラグイン ホストとして別のSnapCenter Serverに追加することはできません。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. 上部の*管理対象ホスト*タブが選択されていることを確認します。
3. *[追加]*をクリックします。
4. [Hosts]ページで、次の操作を実行します。

フィールド	操作
ホストタイプ	ホストのタイプを選択します。 • Windows • Linux  Plug-in for MySQLをMySQLデータベース サーバにインストールする必要があります。

フィールド	操作
ホスト名	通信ホスト名を入力します。ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。SnapCenterが機能するためには、DNSが適切に設定されている必要があります。そのため、FQDNを入力することを推奨します。
Credentials	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。このクレデンシャルには、リモート ホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。  クレデンシャルの認証モードは、[Add Host]ウィザードで指定するホスト タイプによって決まります。

5. [Select Plug-ins to Install]セクションで、インストールするプラグインを選択します。

REST APIを使用してPlug-in for MySQLをインストールする場合は、バージョンを3.0として渡す必要があります。例：MySQL:3.0

6. (オプション) [その他のオプション] をクリックします。

フィールド	操作
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。デフォルトのポート番号は8145です。SnapCenter Serverがカスタム ポートにインストールされている場合は、そのポート番号がデフォルト ポートとして表示されます。  プラグインを手動でインストールしてカスタム ポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理が失敗します。

フィールド	操作
Installation Path	Plug-in for MySQLは、MySQLクライアント ホストにインストールされます。このホストは、Windows システムでもLinuxシステムでもかまいません。 • Windows 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは C:\Program Files\ NetApp\ SnapCenterです。必要に応じて、パスをカスタマイズできます。 • Linux 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは /opt/ NetApp/snapcenter です。必要に応じて、パスをカスタマイズできます。
Skip preinstall checks	プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスをオンにします。
クラスター内のすべてのホストを追加する	該当なし
Use group Managed Service Account (gMSA) to run the plug-in services	該当なし

7. *送信*をクリックします。

[Skip prechecks]チェック ボックスを選択していない場合、プラグインをインストールするための要件をホストが満たしているかどうかを検証するためにホストが検証されます。ディスク スペース、RAM、PowerShellのバージョン、.NETのバージョン、場所（Windowsプラグインの場合）、Javaのバージョン（Linuxプラグインの場合）が最小要件に照らして検証されます。最小要件を満たしていない場合、対応するエラーまたは警告メッセージが表示されます。

エラーがディスク スペースまたはRAMに関連している場合は、C:\Program Files\NetApp\SnapCenter WebAppにあるweb.configファイルを更新してデフォルト値を変更できます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。



HAのセットアップでweb.configファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. ホスト タイプが Linux の場合は、フィンガープリントを確認し、[確認して送信] をクリックします。

クラスタ セットアップでは、クラスタ内の各ノードのフィンガープリントを検証する必要があります。



前述の手順で同じホストがSnapCenterに追加され、フィンガープリントが確認された場合でも、フィンガープリントの検証は必須です。

9. インストールの進捗状況を監視します。

- Windows プラグインの場合、インストールおよびアップグレード ログは次の場所にあります：

C:\Windows\ SnapCenter plugin\Install<JOBID>_

- Linux プラグインの場合、インストール ログは次の場所にあります:
/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install<JOBID>.log_、アップグレード ログ
は次の場所にあります: /var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-
in_Upgrade<JOBID>.log_

終了後の操作

SnapCenter 6.0バージョンにアップグレードすると、既存のPerlベースのPlug-in for MySQLはリモート プラグイン サーバからアンインストールされます。

コマンドレットを使用した複数のリモート ホストへの**SnapCenter Plug-ins Package for Linux / Windows**のインストール

Install-SmHostPackage PowerShellコマンドレットを使用すると、複数のホストにSnapCenter Plug-ins Package for Linux / Windowsを同時にインストールできます。

開始する前に

プラグイン パッケージをインストールする各ホストに対するローカル管理者権限を持つドメイン ユーザとして、SnapCenterにログインしておく必要があります。

手順

1. PowerShellを起動します。
2. SnapCenter Serverホストで、Open-SmConnectionコマンドレットを使用してセッションを確立し、クレデンシャルを入力します。
3. Install-SmHostPackageコマンドレットと必要なパラメータを使用して、複数のホストにプラグインをインストールします。

コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、-skipprecheckオプションを使用できます。

4. リモート インストールのクレデンシャルを入力します。

コマンドライン インターフェイスを使用したLinuxホストへの**SnapCenter Plug-in for MySQL**のインストール

SnapCenter Plug-in for MySQL Databaseは、SnapCenterユーザ インターフェイス (UI) を使用してインストールする必要があります。SnapCenter UIからのプラグインのリモート インストールが許可されていない環境では、コマンドライン インターフェイス (CLI) を使用して、コンソール モードまたはサイレント モードでPlug-in for MySQL Databaseをインストールできます。

開始する前に

- Plug-in for MySQL Databaseは、MySQLインスタンスを保護する必要があるLinuxホストごとにインストールする必要があります。
- SnapCenter Plug-in for MySQL DatabaseをインストールするLinuxホストは、依存するソフトウェア、デ

データベース、オペレーティング システムの要件を満たしている必要があります。

サポートされる構成に関する最新の情報については、Interoperability Matrix Tool (IMT) を参照してください。

"NetApp Interoperability Matrix Tool"

- SnapCenter Plug-in for MySQL Databaseは、SnapCenter Plug-ins Package for Linuxに含まれています。SnapCenter Plug-ins Package for Linuxをインストールする前に、SnapCenterをWindowsホストにインストールしておく必要があります。

手順

1. SnapCenter Plug-ins Package for Linuxのインストール ファイル (snapcenter_linux_host_plugin.bin) をC:\ProgramData\NetApp\SnapCenter\Package RepositoryからPlug-in for MySQLをインストールするホストにコピーします。

このパスには、SnapCenter Serverがインストールされているホストからアクセスできます。

2. コマンド プロンプトから、インストール ファイルをコピーしたディレクトリに移動します。
3. プラグインをインストールします。

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address  
-DSERVER_HTTPS_PORT=port_number_for_server
```

- -DPORT は SMCORE HTTPS 通信ポートを指定します。
- -DSERVER_IP は、 SnapCenter Server の IP アドレスを指定します。
- -DSERVER_HTTPS_PORT は、 SnapCenter Server の HTTPS ポートを指定します。
- -DUSER_INSTALL_DIR は、Linux 用のSnapCenterプラグイン パッケージをインストールするディレクトリを指定します。
- DINSTALL_LOG_NAME はログ ファイルの名前を指定します。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146  
-DUSER_INSTALL_DIR=/opt  
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log  
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. /<インストール ディレクトリ>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties ファイルを編集し、PLUGINS_ENABLED = MySQL:3.0 パラメータを追加します。
5. Add-Smhostコマンドレットと必要なパラメータを使用して、SnapCenter Serverにホストを追加します。

コマンドで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

Plug-in for MySQLのインストール ステータスの監視

[Jobs]ページを使用して、SnapCenterプラグイン パッケージのインストールの進捗状況

を監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、プラグインのインストール操作のみがリストされるようにリストをフィルタリングするには、次の手順を実行します。
 - a. *フィルター*をクリックします。
 - b. オプション：開始日と終了日を指定します。
 - c. [タイプ] ドロップダウン メニューから、[プラグインのインストール] を選択します。
 - d. [Status]ドロップダウン メニューから、インストールのステータスを選択します。
 - e. *適用*をクリックします。
4. インストール ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

CA証明書の設定

CA証明書CSRファイルの生成

証明書署名要求（CSR）を生成し、生成したCSRを使用して認証局（CA）から取得した証明書をインポートできます。証明書には秘密キーが関連付けられます。

CSRはエンコードされたテキストのブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。



CA 証明書の RSA キーの長さは最低 3072 ビットである必要があります。

CSRを生成するための情報については、"[CA証明書CSRファイルの生成方法](#)"。



ドメイン (*.domain.company.com) またはシステム (machine1.domain.company.com) の CA 証明書を所有している場合は、CA 証明書 CSR ファイルの生成をスキップできます。SnapCenterを使用して、既存のCA証明書を導入できます。

クラスタ構成の場合、クラスタ名（仮想クラスタFQDN）と、それぞれのホスト名がCA証明書に記載されている必要があります。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。ワイルドカード証明書 (*.domain.company.com) の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenter ServerとWindowsホスト プラグインにCA証明書をインポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル]>[スナップインの追加と削除] をクリックします。
2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
4. コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書 をクリックします。
5. 「信頼されたルート証明機関」フォルダを右クリックし、[すべてのタスク]>[インポート] を選択して、インポート ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*次へ*をクリックします。
インポート ファイル形式	変更せずに、[次へ] をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、[次へ] をクリックします。
証明書のインポート ウィザードの完了	概要を確認し、[完了] をクリックしてインポートを開始します。



インポートする証明書は秘密キーとバンドルされている必要があります (サポートされている形式は .pfx、.p12、および *.p7b です)。

7. 「個人用」フォルダに対して手順5を繰り返します。

CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための16進数の文字列です。サムプリントは、サムプリント アルゴリズムを使用して証明書の内容から計算されます。

手順

1. GUIで次の手順を実行します。

- a. 証明書をダブルクリックします。
- b. [証明書] ダイアログボックスで、[詳細] タブをクリックします。
- c. フィールドのリストをスクロールして、「拇印」をクリックします。
- d. ボックスから16進数の文字をコピーします。
- e. 16進数の間のスペースを削除します。

たとえば、拇印が「a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b」の場合、スペースを削除すると「a909502dd82ae41433e6f83886b00d4277a32a7b」になります。

2. PowerShellで、次の手順を実行します。

- a. 次のコマンドを実行して、インストールされている証明書のサムプリントを表示し、最近インストールされた証明書をサブジェクト名で識別します。

```
Get-ChildItem -Path 証明書:\LocalMachine\My
```

- b. サムプリントをコピーします。

Windowsホスト プラグイン サービスでのCA証明書の設定

インストールされているデジタル証明書をアクティブ化するには、Windowsホスト プラグイン サービスを使用してCA証明書を設定する必要があります。

SnapCenter Serverと、CA証明書がすでに導入されているすべてのプラグイン ホストで、次の手順を実行します。

手順

1. 次のコマンドを実行して、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

例えば：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

． 次のコマンドを実行して、新しくインストールした証明書をWindowsホスト プラグイン サービスとバインドします。

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例えば：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

LinuxホストでのSnapCenter MySQL Plug-insサービスのCA証明書の設定

インストールされたデジタル証明書をアクティブ化するには、SnapCenterプラグインサービスを使用して、プラグイン キーストアとその証明書のパスワードを管理し、CA証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、`/opt/NetApp/snapcenter/scc/etc`にあるファイル「`keystore.jks`」を使用します。

プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

キー「`KEYSTORE_PASS`」に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
. キーストア内の秘密キー
エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

`agent.properties` ファイルのキー `KEYSTORE_PASS` も同様に更新します。

3. パスワードを変更したら、サービスを再起動します。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは同じである必要があります。

ルート証明書または中間証明書をプラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグイン キーストアが含まれるフォルダーに移動します: /opt/ NetApp/snapcenter/scc/etc。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. ルート証明書か中間証明書を追加します。

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

。ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアにCA署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグイン キーストア /opt/ NetApp/snapcenter/scc/etc が含まれるフォルダーに移動します。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

6. キーストアに追加された新しいCA証明書に対応するエイリアスが、キーストアに含まれていることを確

認めます。

7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのプラグイン キーストア パスワードは、agent.properties ファイルのキー KEYSTORE_PASS の値です。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

・ CA 証明書のエイリアス名が長く、スペースや特殊文字（「*」、「」）が含まれている場合は、エイリアス名を単純な名前に変更します。

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

・ agent.properties ファイルのCA証明書からエイリアス名を設定します。

この値を、キーSCC_CERTIFICATE_ALIASに対して更新します。

8. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

プラグインの証明書失効リスト（CRL）を構成する

タスク概要

- ・ SnapCenterプラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- ・ SnapCenterプラグインの CRL ファイルのデフォルト ディレクトリは、「opt/NetApp/snapcenter/scc/etc/crl」です。

手順

1. キーCRL_PATHに対して、agent.propertiesファイルのデフォルト ディレクトリを変更、更新できます。

このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

WindowsホストでのSnapCenter MySQLプラグイン サービスのCA証明書の設定

インストールされたデジタル証明書をアクティブ化するには、SnapCenterプラグイン サービスを使用して、プラグイン キーストアとその証明書のパスワードを管理し、CA 証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etcにあるファイル keystore.jks を使用します。

プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取

得できます。

これはキー `_KEYSTORE_PASS_` に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```



Windows コマンド プロンプトで「keytool」 コマンドが認識されない場合は、keytool コマンドを完全なパスに置き換えます。

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. キーストア内の秘密キー エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

```
keytool -keypasswd -alias "証明書内のエイリアス名" -keystore keystore.jks
```

`agent.properties` ファイルのキー `KEYSTORE_PASS` も同様に更新します。

4. パスワードを変更したら、サービスを再起動します。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは同じである必要があります。

ルート証明書または中間証明書をプラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc_` に移動します。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. ルート証明書か中間証明書を追加します。

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアにCA署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_` に移動します。
2. ファイル `keystore.jks` を見つけます。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

6. キーストアに追加された新しいCA証明書に対応するエイリアスが、キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのプラグイン キーストア パスワードは、`agent.properties` ファイルのキー `KEYSTORE_PASS` の値です。

```
keytool -keypasswd -alias "CA証明書のエイリアス名" -keystore keystore.jks
```

8. `agent.properties` ファイル内の CA 証明書からエイリアス名を設定します。

この値を、キー `SCC_CERTIFICATE_ALIAS` に対して更新します。

9. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

SnapCenterプラグインの証明書失効リスト（CRL）を構成する

タスク概要

- 関連するCA証明書の最新のCRLファイルをダウンロードするには、["SnapCenter CA証明書の証明書失効リストファイルを更新する方法"](#)。
- SnapCenterプラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- SnapCenterプラグインの CRL ファイルのデフォルト ディレクトリは、`'C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'` です。

手順

1. キー `CRL_PATH` に対して、`agent.properties` ファイル内のデフォルト ディレクトリを変更および更新できます。
2. このディレクトリには、複数のCRLファイルを格納できます。

受信する証明書については、それぞれのCRLに対して検証が行われます。

プラグインのCA証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインでCA証明書の検証を有効にする必要があります。

開始する前に

- 実行 `Set-SmCertificateSettings` コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- `Get-SmCertificateSettings` を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで使用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. プラグイン ホストを1つまたは複数選択します。
4. *その他のオプション*をクリックします。
5. *証明書の検証を有効にする*を選択します。

終了後の操作

[Managed Hosts]タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Serverとプラグイン ホスト間の接続のステータスを示します。

- ** は、CA 証明書が有効になっていないか、プラグイン ホストに割り当てられていないことを示します。
- ** は CA 証明書が正常に検証されたことを示します。
- ** は、CA 証明書を検証できなかったことを示します。
- ** は接続情報を取得できなかったことを示します。



ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

データ保護の準備

SnapCenter Plug-in for MySQLを使用するための前提条件

ユーザがSnapCenter Plug-in for MySQLを使用するためには、SnapCenter管理者が事前にSnapCenter Serverをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter Serverをインストールして設定します。
- SnapCenter Serverにログインします。
- SnapCenter環境を設定するために、必要に応じて、ストレージ システム接続を追加し、クレデンシャル

を作成します。

- LinuxホストまたはWindowsホストにJava 11をインストールします。

Javaパスは、ホスト マシンの環境パス変数で設定する必要があります。

- バックアップ レプリケーションが必要である場合は、SnapMirrorとSnapVaultをセットアップします。

MySQLの保護におけるソース、リソース グループ、ポリシーの使用方法

SnapCenterを使用する前に、実行するバックアップ、クローニング、リストアの各処理に関連する基本的な概念を理解しておくに役立ちます。ここでは、これらの処理で扱うリソース、リソース グループ、およびポリシーについて説明します。

- リソースとは、一般にはSnapCenterでバックアップまたはクローニングするMySQLインスタンスのことです。
- SnapCenterリソース グループは、ホスト上のリソースの集まりです。

リソース グループに対して処理を実行すると、リソース グループに指定したスケジュールに従って、リソース グループに定義されているリソースに対して処理が実行されます。

単一のリソースまたはリソース グループをオンデマンドでバックアップすることができます。また、スケジュールされたバックアップを単一リソースおよびリソース グループに対して実行することもできます。

- ポリシーは、バックアップ頻度、レプリケーション、スクリプトといった、データ保護処理の特性を指定するものです。

リソース グループを作成するときに、そのグループに対して1つ以上のポリシーを選択します。単一リソースに対してオンデマンドでバックアップを実行するときにもポリシーを選択できます。

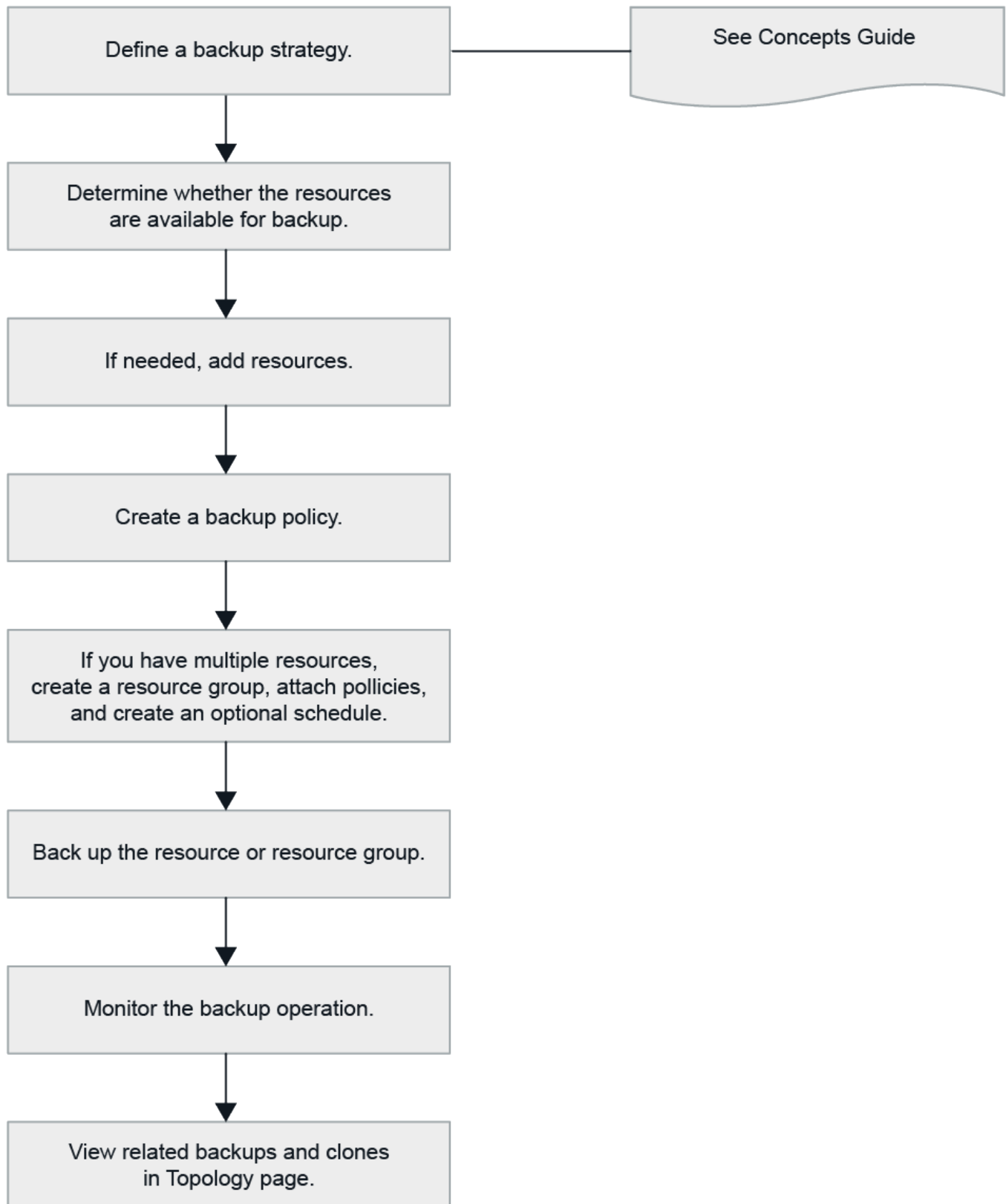
リソース グループでは、保護する対象と保護するタイミング（日時）を定義できます。ポリシーでは、保護する方法を定義できます。たとえば、すべてのデータベースをバックアップする場合は、ホストのすべてのデータベースを含むリソース グループを作成します。このリソース グループに、日次ポリシーと毎時ポリシーの2つのポリシーを適用します。リソース グループを作成してポリシーを適用する際に、フル バックアップを1日1回実行するようにリソース グループを設定できます。

MySQLリソースのバックアップ

MySQLリソースのバックアップ

リソース（データベース）またはリソース グループのバックアップを作成することができます。バックアップのワークフローには、計画、バックアップするデータベースの特定、バックアップ ポリシーの管理、リソース グループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

次のワークフローは、バックアップ処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトでを使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。<https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html>["SnapCenterソフトウェア コマンドレット リファレンス ガイド"^]。

データベースの自動的検出

リソースとは、SnapCenterで管理するLinuxホスト上のMySQLデータベースです。使用できるMySQLデータベースを検出したあとに、それらのリソースをリソース グループに追加してデータ保護処理を実行できます。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の作成などのタスクを事前に完了しておく必要があります。
- SnapCenter Plug-in for MySQLでは、RDM / VMDK仮想環境にあるリソースの自動検出がサポートされていません。データベースを手動で追加する際に、仮想環境のストレージの情報を指定する必要があります。

タスク概要

- プラグインをインストールすると、そのLinuxホスト上のすべてのデータベースが自動検出されて[Resources]ページに表示されます。
- 自動検出されるのはデータベースだけです。

自動検出されたリソースを変更または削除することはできません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから MySQL 用プラグインを選択します。
2. [Resources] ページで、[View] リストからリソース タイプを選択します。
3. (オプション) をクリック 、ホスト名を選択します。

をクリックします  フィルター パネルを閉じます。

4. ホスト上で利用可能なリソースを検出するには、[リソースの更新] をクリックします。

リソースは、リソース タイプ、ホスト名、関連するリソース グループ、バックアップ タイプ、ポリシー、全体的なステータスなどの情報とともに表示されます。

- データベースがNetAppストレージにあって保護されていない場合は、[Overall Status]列に「Not protected」と表示されます。
- データベースがNetAppストレージ システム上にあって保護されており、バックアップ処理が実行されていない場合は、[Overall Status]列に「Backup not run is displayed」と表示されます。それ以外の場合は、前回のバックアップ ステータスに基づいて、ステータスが「バックアップに失敗しました」または「バックアップに成功しました」に変わります。



SnapCenterの外部でインスタンスの名前が変更された場合は、リソースを更新する必要があります。

手動でのプラグイン ホストへのリソースの追加

自動検出はWindowsホストではサポートされていません。MySQLインスタンスとデータベース リソースは手動で追加する必要があります。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の設定などのタスクを完了しておく必要があります。

手順

1. 左側のナビゲーション ペインで、ドロップダウン リストから MySQL 用のSnapCenterプラグインを選択し、リソース をクリックします。
2. リソース ページで、*MySQL リソースの追加*をクリックします。
3. [Provide Resource Details]ページで、次の操作を実行します。

フィールド	操作
Name	データベース名を指定します。
Host Name	ホスト名を入力します。
タイプ	インスタンスを選択します。
Instance	該当なし。
Credentials	クレデンシャルを選択するか、クレデンシャルの情報を追加します。 これはオプションです。

4. [ストレージ フットプリントの提供] ページで、ストレージ タイプを選択し、1 つ以上のボリューム、LUN、および qtree を選択して、[保存] をクリックします。

オプション：をクリックすることもできます  アイコンをクリックして、他のストレージ システムからボリューム、LUN、qtree を追加します。

5. オプション: リソース設定ページで、MySQL プラグインのカスタム キーと値のペアを入力します。
6. 概要を確認し、[完了] をクリックします。

データベースは、ホスト名、関連するリソース グループとポリシー、全体的なステータスなどの情報とともに表示されます。

リソースへのアクセスをユーザに許可する場合は、ユーザにリソースを割り当てる必要があります。これにより、ユーザは、自身に割り当てられたアセットに対して、権限のある処理を実行できるようになります。

"ユーザまたはグループの追加と、ロールとアセットの割り当て"

データベースの追加が完了したら、MySQLデータベースの詳細を変更できます。

MySQLのバックアップ ポリシーの作成

SnapCenterを使用してMySQLリソースをバックアップする前に、バックアップ対象のリソースまたはリソース グループのバックアップ ポリシーを作成する必要があります。バックアップ ポリシーとは、バックアップをどのように管理し、スケジューリングし、保持するかを定める一連のルールです。

開始する前に

- バックアップ戦略を定義しておく必要があります。

詳細については、MySQLデータベースのデータ保護戦略の定義に関する説明を参照してください。

- SnapCenterのインストール、ホストの追加、ストレージ システム接続の作成、リソースの追加などのタスクを実行して、データ保護の準備をしておく必要があります。
- ユーザがSnapshotをミラーまたはバックアップにレプリケートする場合は、ソース ボリュームとデスティネーション ボリューム両方のSVMをSnapCenter管理者がユーザに割り当てる必要があります。

ポリシーで、レプリケーション、スクリプト、アプリケーション設定を指定することもできます。それらのオプションを指定しておくことで、別のリソース グループにポリシーを再利用して時間を節約することができます。

タスク概要

- SnapLock
 - [Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで指定した保持日数以下にする必要があります。
 - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、ポリシーで指定した数よりも多くのSnapshotが保持される可能性があります。
 - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[ポリシー]をクリックします。
3. *新規*をクリックします。
4. 「名前」 ページで、ポリシー名と詳細を入力します。
5. [Policy type]ページで、次の手順を実行します。
 - a. ストレージ タイプを選択します。
 - b. カスタム バックアップ設定セクションでは、キーと値の形式でプラグインに渡す必要がある特定のバックアップ設定を指定します。

プラグインに渡すキーと値のペアを複数指定することができます。

6. スナップショットとレプリケーション ページで、次の手順を実行します。

- a. オンデマンド、時間別、日次、週次、または*月次*を選択してスケジュール タイプを指定します。



リソース グループを作成する際に、バックアップ処理のスケジュール（開始日、終了日、頻度）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソース グループを作成できますが、各ポリシーに異なるバックアップ スケジュールを割り当てることもできます。



午前 2 時にスケジュールを設定した場合、夏時間 (DST) 中はスケジュールは実行されません。

- a. スナップショット設定セクションで、バックアップ タイプ ページで選択したバックアップ タイプとスケジュール タイプの保持設定を指定します。

状況	操作
特定の数のSnapshotを保持	*保持するコピー*を選択し、保持するスナップショットの数を指定します。 Snapshotの数が指定した数を超えると、古いものから順にSnapshotが削除されます。 SnapVaultレプリケーションを有効にする場合は、保持数を2以上に設定する必要があります。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。 最大保持値は 1018 です。保持数を、使用しているONTAPバージョンがサポートする値よりも大きい値に設定すると、バックアップが失敗します。
Snapshotを特定の日数だけ保持	*コピーの保持期間*を選択し、スナップショットを削除する前に保持する日数を指定します。
スナップショットコピーのロック期間	スナップショット コピーのロック期間 を選択し、日、月、または年を指定します。 SnapLock保持期間は100年未満にする必要があります。

- b. ポリシーラベルを選択します。



リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしながらでも実行できます。

7. [セカンダリ レプリケーション オプションの選択] セクションで、次のセカンダリ レプリケーション オプションの 1 つまたは両方を選択します。

フィールド	操作
ローカル スナップショット コピーを作成した後、 SnapMirror を更新します	別のボリュームにバックアップ セットのミラー コピーを作成する場合（SnapMirrorレプリケーション）は、このフィールドを選択します。 ONTAPの保護関係のタイプがミラーとバックアップの場合、このオプションのみを選択すると、プライマリで作成されたSnapshotがデスティネーションに転送されませんが、デスティネーションのリストに表示されます。このスナップショットを復元操作を実行するために宛先から選択すると、次のエラー メッセージが表示されます: 選択したボールド/ミラー バックアップにはセカンダリ ロケーションは使用できません。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。 トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 見る"トポロジページでMySQLリソース関連のバックアップとクローンを表示します。"。

フィールド	操作
ローカルスナップショットコピーを作成した後、 SnapVault を更新します	ディスクツーディスクのバックアップ レプリケーション（SnapVaultバックアップ）を実行する場合は、このオプションを選択します。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 SnapLock がSnapLock Vault と呼ばれるONTAPのセカンダリにのみ設定されている場合、[トポロジ] ページの [更新] ボタンをクリックすると、ONTAPから取得されたセカンダリのロック期間が更新されます。 SnapLock Vault の詳細については、「Vault の保存先でスナップショットを WORM にコミットする」を参照してください。 見る"トポロジページでMySQLリソース関連のバックアップとクローンを表示します。"。
エラー再試行回数	処理が停止されるまでに試行できるレプリケーションの最大回数を入力します。



セカンダリ ストレージでSnapshotの上限に達しないように、ONTAPでセカンダリ ストレージのSnapMirror保持ポリシーを設定する必要があります。

8. 概要を確認し、[完了] をクリックします。

リソース グループの作成とポリシーの適用

リソース グループはコンテナであり、バックアップして保護するリソースをここに追加する必要があります。リソース グループを使用することで、特定のアプリケーションに関連するすべてのデータを同時にバックアップできます。リソース グループはいずれのデータ保護ジョブにも必要になります。リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義することも必要です。

タスク概要

- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。

2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。

フィールド	操作
Name	リソース グループの名前を入力します。  リソース グループ名は250文字以内で指定する必要があります。
Tags	リソース グループを検索しやすくするために、ラベルを入力します。 たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。
Use custom name format for snapshot copy	Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。 たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

4. [リソース] ページで、[ホスト] ドロップダウン リストからホスト名を選択し、[リソース タイプ] ドロップダウン リストからリソース タイプを選択します。

画面の情報がフィルタリングされます。

5. *利用可能なリソース*セクションからリソースを選択し、右矢印をクリックして*選択したリソース*セクションに移動します。
6. [Application Settings] ページで、次の操作を実行します。

- a. 追加のバックアップ オプションを設定するには、[バックアップ] 矢印をクリックします。

整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for Consistency Group snapshot operation to complete	スナップショット操作が完了するまでの待機時間を指定するには、「緊急」、「中」、または「緩和」を選択します。 [Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。

フィールド	操作
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

+

- *スクリプト*矢印をクリックし、静止、スナップショット、および静止解除操作の事前および事後コマンドを入力します。障害の発生時に終了前に実行するプリコマンドも入力できます。
- *カスタム構成*矢印をクリックし、このリソースを使用するすべてのデータ保護操作に必要なカスタムのキーと値のペアを入力します。

パラメータ	設定	説明
ARCHIVE_LOG_ENABLE	(Y / N)	アーカイブ ログ管理を有効にし、アーカイブ ログを削除します。
ARCHIVE_LOG_RETENTION	number_of_days	アーカイブ ログを保持する日数を指定します。 この設定は、NTAP_SNAPSHOT_RETENTIONS 以上である必要があります。
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブ ログが含まれるディレクトリへのパスを指定します。

パラメータ	設定	説明
ARCHIVE_LOG_EXT	file_extension	アーカイブ ログ ファイルの拡張子の長さを指定します。 たとえば、アーカイブ ログが log_backup_0_0_0_0.161518551942 9 で、file_extension 値が 5 の場合、ログの拡張子は 5 桁、つまり 16151 になります。
ARCHIVE_LOG_RECURSIVE_SE ARCH	(Y / N)	サブディレクトリ内のアーカイブ ログの管理を有効にします。 アーカイブ ログがサブディレクトリの下にある場合は、このパラメータを使用する必要があります。



カスタムのキーと値のペアは、MySQL Linuxプラグイン システムではサポートされませんが、一元化されたWindowsプラグインとして登録されたMySQLデータベースではサポートされません。

- c. スナップショット コピー ツール の矢印をクリックして、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する（このオプションはLinuxリソースには適用されません）	ファイル システムの一貫性を備えたSnapCenter * を選択します。
SnapCenterでストレージ レベルのSnapshotを作成する	ファイル システムの整合性のないSnapCenter * を選択します。
Snapshotを作成するためにホストで実行するコマンドを入力する	*その他*を選択し、スナップショットを作成するためにホスト上で実行するコマンドを入力します。

7. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます 。

ポリシーが[Configure schedules for selected policies]セクションのリストに表示されます。

- b. スケジュールの設定列で*をクリックします。  * 設定するポリシーの。
- c. ポリシー *policy_name* のスケジュールの追加ダイアログ ボックスでスケジュールを構成し、[OK] をクリックします。

*policy_name*は、選択したポリシーの名前です。

構成されたスケジュールは、「適用されたスケジュール」列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP サーバーは、設定 > グローバル設定 で設定する必要があります。

9. 概要を確認し、[完了] をクリックします。

リソース グループを作成し、**ASA r2** システム上の **MySQL** リソースの二次保護を有効にする

ASA r2 システム上にあるリソースを追加するには、リソース グループを作成する必要があります。リソース グループの作成時にセカンダリ保護をプロビジョニングすることもできます。

開始する前に

- ONTAP 9.x リソースとASA r2 リソースの両方を同じリソース グループに追加していないことを確認する必要があります。
- ONTAP 9.x リソースとASA r2 リソースの両方を含むデータベースが存在しないことを確認する必要があります。

タスク概要

- 二次保護は、ログインしたユーザーに **SecondaryProtection** 機能が有効になっているロールが割り当てられている場合にのみ使用できます。
- セカンダリ保護を有効にすると、プライマリおよびセカンダリ整合性グループの作成中にリソース グループはメンテナンス モードになります。プライマリおよびセカンダリのコンシステンシー グループが作成されると、リソース グループのメンテナンス モードが解除されます。
- SnapCenter はクローン リソースの二次保護をサポートしていません。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name]ページで、次の操作を実行します。
 - a. [Name]フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag]フィールドに1つ以上のラベルを入力します。

たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

- c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

たとえば、`customtext_resource group_policy_hostname`や`resource group_hostname`などの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- d. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。



必要に応じて、プレフィックスを含め、アプリケーションで設定されたのと同じ宛先を使用する必要があります。

4. [リソース] ページで、[ホスト] ドロップダウン リストからデータベース ホスト名を選択します。



[Available Resources]セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources]のリストには表示されません。

5. [使用可能なリソース] セクションからASA r2 リソースを選択し、[選択したリソース] セクションに移動します。
6. アプリケーション設定ページで、バックアップ オプションを選択します。
7. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックし  てポリシーを作成することもできます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、  をクリックします。
- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 選択したポリシーに対して二次保護が有効になっている場合は、「二次保護」 ページが表示されるので、次の手順を実行する必要があります。

- a. レプリケーション ポリシーのタイプを選択します。



同期レプリケーション ポリシーはサポートされていません。

- b. 使用する整合性グループのサフィックスを指定します。

- c. [宛先クラスタ] および [宛先 SVM] ドロップダウンから、使用するピア クラスタと SVM を選択します。



クラスタと SVM のピアリングはSnapCenterではサポートされていません。クラスタと SVM のピアリングを実行するには、System Manager またはONTAP CLI を使用する必要があります。



リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは [セカンダリ保護リソース] セクションに表示されます。

1. [Verification] ページで、次の手順を実行します。

- a. ロケーターのロード をクリックして、 SnapMirrorまたはSnapVaultボリュームをロードし、セカンダリストレージで検証を実行します。
- b. クリック  ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で をクリックします。
- c. [Add Verification Schedules policy_name] ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

- d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証] を選択します。
- e. [OK] をクリックします。

設定した検証スケジュールが、[Applied Schedules] 列にリストされます。

2. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtptServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

3. 概要を確認し、[完了] をクリックします。

MySQL用のPowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成

PowerShellコマンドレットを使用してMySQLデータベースのバックアップ、リストア、クローニングを行う前に、Storage Virtual Machine (SVM) 接続とクレデンシャルを作成する必要があります。

開始する前に

- PowerShellコマンドレットを実行できるようにPowerShell環境を準備しておく必要があります。
- ストレージ接続を作成するには、Infrastructure Adminロールの権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

ストレージ システム接続の追加中は、ホスト プラグインのインストールが進行中であってはなりません。ホスト キャッシュが更新されず、SnapCenter GUI にデータベースのステータスが「バックアップに使用できません」または「NetAppストレージ上にありません」と表示される可能性があるためです。

- ストレージ システムの名前は一意である必要があります。

SnapCenterでは、別々のクラスタに属している場合でも、複数のストレージ システムに同じ名前を付けることはサポートされません。SnapCenterでサポートする各ストレージ システムには、一意な名前とデータLIFの一意なIPアドレスが必要です。

手順

1. Open-SmConnectionコマンドレットを使用して、PowerShell Core接続セッションを開始します。

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

2. Add-SmStorageConnectionコマンドレットを使用して、ストレージ システムへの新しい接続を作成します。

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Add-SmCredentialコマンドレットを使用して、新しいクレデンシャルを作成します。

この例は、Windowsクレデンシャルを使用してFinanceAdminという名前の新しいクレデンシャルを作成する方法を示しています。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. SnapCenter ServerにMySQL通信ホストを追加します。


```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName FinanceAdmin -PluginCode mysql
```

5. パッケージとSnapCenter Plug-in for MySQLをホストにインストールします。

Linux :

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode mysql
```

Windows :

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode mysql  
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. SQLLIBのパスを設定します。

Windows の場合、MySQL プラグインは SQLLIB フォルダのデフォルト パス「C:\Program Files\IBM\SQLLIB\BIN」を使用します。

デフォルト パスを上書きする場合は、次のコマンドを使用します。

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode MySQL -configSettings @{ "MySQL_SQLLIB_CMD" = "  
    "<custom_path>\IBM\SQLLIB\BIN"
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

MySQLのバックアップ

どのリソース グループにもまだ含まれていないリソースは、[Resources]ページからバックアップすることができます。

開始する前に

- バックアップ ポリシーを作成しておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。
- Snapshotコピーベースのバックアップ処理の場合は、すべてのテナント データベースが有効でアクティブであることを確認してください。
- 休止、Snapshot、および休止解除の処理を実行するプリコマンドとポストコマンドの場合は、プラグイン

ホストで次のパスから使用できるコマンド リストにコマンドがあるかどうかを確認する必要があります。

- Windows ホスト上のデフォルトの場所: `C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux ホスト上のデフォルトの場所: `/opt/ NetApp/ snapcenter/ scc/ etc/ allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. リソース ページで、リソース タイプに基づいて 表示 ドロップダウン リストからリソースをフィルターします。

を選択 、ホスト名とリソース タイプを選択して、リソースをフィルターします。次に選択できます  フィルター パネルを閉じます。

3. バックアップするリソースを選択します。
4. [リソース] ページで、[スナップショット コピーにカスタム名形式を使用する] を選択し、スナップショット名に使用するカスタム名形式を入力します。

たとえば、*customtext_policy_hostname* または *resource_hostname* です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

5. [Application Settings] ページで、次の操作を実行します。

- 追加のバックアップ オプションを設定するには、[バックアップ] 矢印を選択します。

必要に応じて、整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for "Consistency Group Snapshot" operation to complete	スナップショット操作が完了するまでの待機時間を指定するには、「緊急」、または「中」、または「緩和」を選択します。[Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

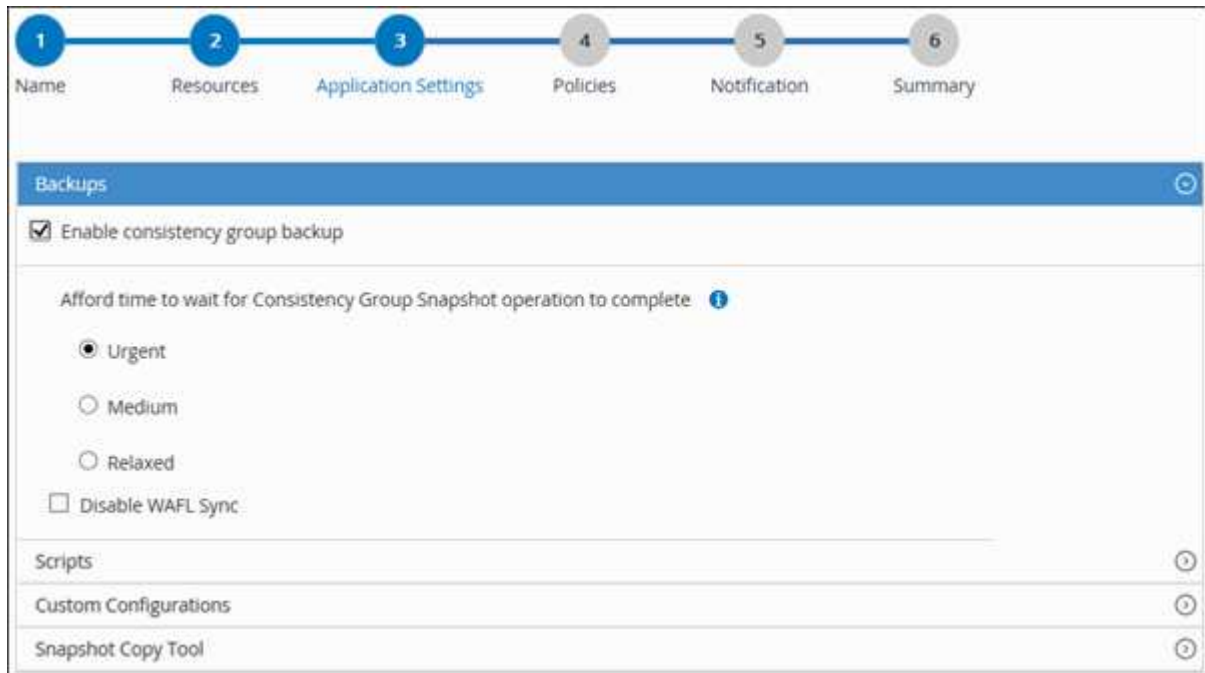
- *スクリプト*矢印を選択して、静止、スナップショット、および静止解除操作の事前および事後コマンドを実行します。

バックアップ処理を終了する前のプリコマンドも実行できます。プリスクリプトとポストスクリプトはSnapCenter Serverで実行されます。

- カスタム構成矢印を選択し、このリソースを使用するすべてのジョブに必要なカスタム値のペアを入力します。
- スナップショット コピー ツール 矢印を選択して、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでストレージ レベルのSnapshotを作成する	• ファイル システムの整合性のないSnapCenter * を選択します。

あなたが望むなら...	操作
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する	ファイル システムの一貫性を備えたSnapCenter * を選択します。
Snapshotを作成するためのコマンドを入力する	*その他*を選択し、スナップショットを作成するコマンドを入力します。



6. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックしてポリシーを作成することもできます 。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b.  を選択
スケジュールを構成するポリシーの [スケジュールの構成] 列で、
- c. ポリシー *policy_name* のスケジュールの追加 ダイアログ ボックスでスケジュールを構成し、[OK] を選択します。

policy_name は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

7. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。

す。SMTP は、設定 > グローバル設定 でも設定する必要があります。

8. 概要を確認し、[完了] を選択します。

リソースのトポロジ ページが表示されます。

9. *今すぐバックアップ*を選択します。

10. [Backup]ページで次の手順を実行します。

- a. リソースに複数のポリシーを適用した場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*を選択します。

11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

- MetroCluster構成では、フェイルオーバー後にSnapCenterで保護関係を検出できないことがあります。

詳細については、以下を参照してください。 ["MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"](#)

- VMDK上のアプリケーション データをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープ サイズが不足していると、バックアップが失敗することがあります。

Java ヒープ サイズを増やすには、スクリプト ファイル `/opt/netapp/init_scripts/scvservice` を見つけます。このスクリプトでは、`do_start method` コマンドによってSnapCenter VMware プラグイン サービスが開始されます。このコマンドを次のように更新します: `Java -jar -Xmx8192M -Xms4096M`

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-SmConnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\\
```

ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmResourcesコマンドレットを使用して、手動リソースを追加します。

次の例は、MySQLインスタンスを追加する方法を示しています。

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode MySQL
-ResourceType Instance -ResourceName mysqlinst1 -StorageFootPrint
(@{"VolumeName"="winmysql01_data01";"LUNName"="winmysql01_data01";"S
torageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Add-SmPolicyコマンドレットを使用して、バックアップ ポリシーを作成します。
4. リソースを保護するか、Add-SmResourceGroupコマンドレットを使用してSnapCenterに新しいリソース グループを追加します。
5. New-SmBackupコマンドレットを使用して、新しいバックアップ ジョブを開始します。

この例は、リソース グループをバックアップする方法を示しています。

```
C:\PS> New-SmBackup -Resources
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306";"P
luginName"="MySQL"} -Policy "MySQL_snapshotbased"
```

この例では、保護されたリソースをバックアップしています。

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
-Policy mysql_policy2
```

6. Get-smJobSummaryReportコマンドレットを使用して、ジョブのステータス（実行中、完了、失敗）を確認します。

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Get-SmBackupReportコマンドレットを使用して、リストアやクローニングの処理を実行するバックアップIDとバックアップ名など、バックアップ ジョブの詳細を監視します。

```

PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :

```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

リソース グループのバックアップ

リソース グループは、ホスト上のリソースの集まりです。リソース グループのバックアップ処理は、リソース グループに定義されているすべてのリソースを対象に実行されます。

開始する前に

- ポリシーを適用したリソース グループを作成しておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。

タスク概要

リソース グループは、[Resources]ページからオンデマンドでバックアップできます。リソース グループにポ

リシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが行われます。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。

リソースグループを検索するには、検索ボックスにリソースグループ名を入力するか、 をクリックして、タグを選択します。次に選択できます  フィルター パネルを閉じます。

3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] を選択します。
4. [Backup] ページで次の手順を実行します。
 - a. リソース グループに複数のポリシーを関連付けた場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*を選択します。

5. モニター > ジョブ を選択して、操作の進行状況を監視します。

MySQLのバックアップ処理の監視

SnapCenterの[Jobs]ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*ジョブ*をクリックします。
3. [Jobs]ページで、次の手順を実行します。

- a. をクリックして、 リストの内容をバックアップ処理だけに絞り込みます。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*バックアップ*を選択します。
 - d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. バックアップ ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスは  ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[Activity]ペインでのMySQLインスタンスのデータ保護処理の監視

[Activity]ペインには、最後に実行された5つの処理が表示されます。また[Activity]ペインには、処理が開始された日次と処理のステータスが表示されます。

[Activity]ペインには、バックアップ、リストア、クローニング、スケジュールされたバックアップの各処理に関する情報が表示されます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. クリック  アクティビティ ペインで、最新の 5 つの操作を表示します。

いずれかの操作をクリックすると、*ジョブの詳細*ページに操作の詳細が表示されます。

MySQLのバックアップ処理のキャンセル

キューに登録されているバックアップ処理はキャンセルできます。

必要なもの

- 処理をキャンセルするには、SnapCenter管理者かジョブ所有者としてログインする必要があります。
- バックアップ操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のバックアップ処理はキャンセルできません。
- バックアップ処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。
- キャンセルできない操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたバックアップ操作をキャンセルできます。

手順

1. 次のいずれかを実行します。

方法	アクション
[Monitor]ページ	a. 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 b. 操作を選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	a. バックアップ操作を開始したら、*をクリックします。 * アクティビティ ペインで、最新の 5 つの操作を表示します。 b. 処理を選択します。 c. ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

処理がキャンセルされ、リソースは処理前の状態に戻ります。

[Topology]ページでのMySQLのバックアップとクローンの表示

リソースのバックアップまたはクローニングを準備する際に、プライマリ ストレージとセカンダリ ストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。

タスク概要

プライマリ ストレージまたはセカンダリ ストレージ（ミラー コピーまたはバックアップ コピー）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

-  プライマリ ストレージで使用可能なバックアップとクローンの数を表示します。
-  SnapMirrorテクノロジーを使用してセカンダリ ストレージにミラーリングされているバックアップとクローンの数を表示します。
-  SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップとクローンの数を表示します。



表示されるバックアップの数には、セカンダリ ストレージから削除されたバックアップも含まれます。たとえば、バックアップを4個保持するポリシーを使用してバックアップを6個作成した場合、バックアップの数は6個と表示されます。



mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジビューに表示されますが、トポロジビューのミラーバックアップの数にはバージョンに依存しないバックアップは含まれません。

[Topology]ページでは、選択したリソースまたはリソースグループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を参照し、対象を選択してデータ保護処理を実行できます。

手順

1. 左側のナビゲーションペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウンリストからリソースまたはリソースグループを選択します。
3. リソースの詳細ビューまたはリソースグループの詳細ビューで、リソースを選択します。

リソースが保護されている場合は、選択したリソースのトポロジページが表示されます。

4. *概要カード*を確認して、プライマリストレージとセカンダリストレージで使用可能なバックアップとクローンの数の概要を確認します。

概要カードセクションには、スナップショットコピーベースのバックアップとクローンの合計数が表示されます。

更新ボタンをクリックすると、ストレージのクエリが開始され、正確な数が表示されます。

SnapLock対応バックアップが取得された場合、[更新] ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでも、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

アプリケーションリソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限はONTAPから取得されます。

オンデマンドバックアップ後、[更新] ボタンをクリックすると、バックアップまたはクローンの詳細が更新されます。

5. 「コピーの管理」ビューで、プライマリストレージまたはセカンダリストレージからバックアップまたはクローンをクリックして、バックアップまたはクローンの詳細を表示します。

バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、削除の各処理を実行します。



セカンダリストレージ上のバックアップは、名前変更または削除できません。

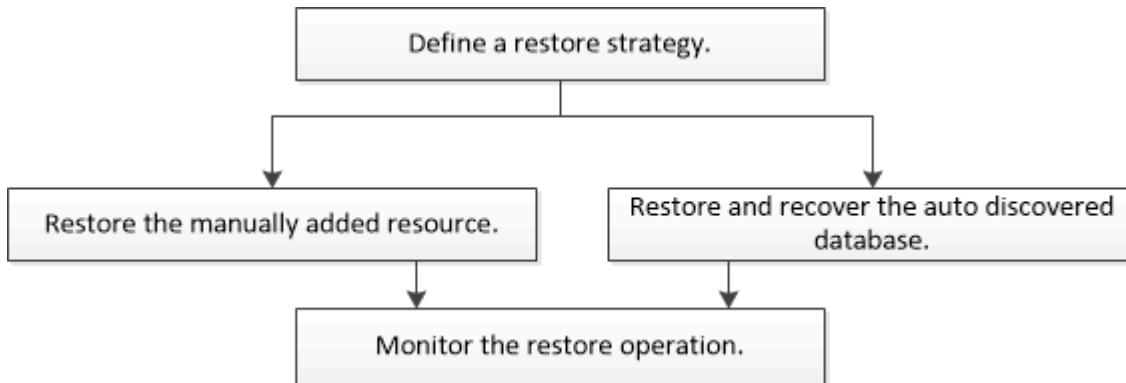
7. クローンを削除する場合は、表でクローンを選択し、 をクリックします。
8. クローンを分割する場合は、テーブルからクローンを選択し、。

MySQLのリストア

リストアのワークフロー

リストアとリカバリのワークフローには、計画、リストア処理の実行、および処理の監視が含まれます。

次のワークフローは、リストア処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

手動で追加されたリソース バックアップのリストアとリカバリ

SnapCenterを使用して1つまたは複数のバックアップからデータをリストアおよびリカバリすることができます。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- リストアするリソースまたはリソース グループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- リストア前、リストア後、マウント、アンマウントの各コマンドを実行する場合は、プラグイン ホストで次のパスから使用可能なコマンド リストにコマンドが存在するかどうかを確認する必要があります。
 - Windows ホスト上のデフォルトの場所: `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux ホスト上のデフォルトの場所: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- ONTAP 9.12.1 以前のバージョンでは、復元の一環としてSnapLock Vault スナップショットから作成されたクローンには、 SnapLock Vault の有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホスト、関連するリソース グループとポリシー、およびステータスとともに表示されます。



リストアの実行時は、バックアップがリストア グループに対するものであっても、リストア対象のリソースを個別に選択する必要があります。

リソースが保護されていない場合は、「全体ステータス」列に「保護されていません」と表示されます。この状態になるのは、リソースが保護されていない場合とリソースが別のユーザによってバックアップされている場合です。

3. リソースを選択するか、リソース グループを選択してそのグループ内のリソースを選択します。

リソースのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージ システムから [バックアップ] を選択します。
5. プライマリバックアップテーブルで、復元するバックアップを選択し、*をクリックします。  *。

Primary Backup(s)	
search 	  
Backup Name	End Date
rg1_scspr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. 復元範囲ページで、*完全なリソース*を選択します。

- a. *完全なリソース*を選択すると、MySQL データベースのすべての構成済みデータ ボリュームが復元されます。

リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeのリストア用のSnapshotが選択されたあとに作成されたSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。

複数のLUNを選択できます。



すべて を選択すると、ボリューム、qtree、または LUN 上のすべてのファイルが復元されます。

7. [Pre ops] ページで、リストア ジョブの実行前に実行するリストア前の処理とアンマウントのコマン

ドを入力します。

自動検出されたリソースにはアンマウント コマンドを使用できません。

8. [Post ops]ページで、リストア ジョブの実行後に実行するマウントとリストア後の処理のコマンドを入力します。

自動検出されたリソースにはマウント コマンドを使用できません。

9. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP は、[設定] > [グローバル設定] ページでも設定する必要があります。

10. 概要を確認し、[完了] をクリックします。

11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよびGet-SmBackupReportコマンドレットを使用して、リストアする1つまたは複数のバックアップに関する情報を取得します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackup コマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

自動検出されたデータベース バックアップのリストアとリカバリ

SnapCenterを使用して1つまたは複数のバックアップからデータをリストアおよびリカバリすることができます。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- リストアするリソースまたはリソース グループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。
- リストア前、リストア後、マウント、アンマウントの各コマンドを実行する場合は、プラグイン ホストで次のパスから使用可能なコマンド リストにコマンドが存在するかどうかを確認する必要があります。

- Windows ホスト上のデフォルトの場所: `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux ホスト上のデフォルトの場所: `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。

タスク概要

- 自動検出されたリソースについては、SFSRでリストアがサポートされます。
- ポイントインタイムおよび最新の状態への自動リカバリはサポートされていません。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホスト、関連するリソース グループとポリシー、およびステータスとともに表示されます。



リストアの実行時は、バックアップがリストア グループに対するものであっても、リストア対象のリソースを個別に選択する必要があります。

リソースが保護されていない場合は、「全体ステータス」列に「保護されていません」と表示されます。この状態になるのは、リソースが保護されていない場合とリソースが別のユーザによってバックアップされている場合です。

3. リソースを選択するか、リソース グループを選択してそのグループ内のリソースを選択します。

リソースのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージシステムから [バックアップ] を選択します。
5. プライマリバックアップテーブルで、復元するバックアップを選択し、*をクリックします。  *

Primary Backup(s)	
search 	  
Backup Name	End Date
rg1_scspr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. 「復元範囲」 ページで、「完全なリソース」を選択して、MySQL データベースの構成済みデータ ボリュームを復元します。
7. [Pre ops] ページで、リストア ジョブの実行前に実行するリストア前の処理とアンマウントのコマンドを入

力します。

自動検出されたリソースにはアンマウント コマンドを使用できません。

8. [Post ops] ページで、リストア ジョブの実行後に実行するマウントとリストア後の処理のコマンドを入力します。

自動検出されたリソースにはマウント コマンドを使用できません。

9. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP は、[設定] > [グローバル設定] ページでも設定する必要があります。

10. 概要を確認し、[完了] をクリックします。
11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレットを使用したリソースのリストア

リソースのバックアップをリストアするときは、SnapCenter Serverとの接続セッションを開始し、バックアップをリストしてバックアップの情報を取得し、バックアップをリストアします。

PowerShellコマンドレットを実行できるように環境を準備しておく必要があります。

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよびGet-SmBackupReportコマンドレットを使用して、リストアする1つまたは複数のバックアップに関する情報を取得します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime
"2/3/2015"

SmBackupId           : 113
SmJobId               : 2032
StartDateTime        : 2/2/2015 6:57:03 AM
EndDateTime          : 2/2/2015 6:57:11 AM
Duration              : 00:00:07.3060000
CreatedDateTime       : 2/2/2015 6:57:23 AM
Status               : Completed
ProtectionGroupName  : Clone
SmProtectionGroupId   : 34
PolicyName            : Vault
SmPolicyId            : 18
BackupName            : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus    : NotVerified

SmBackupId           : 114
SmJobId               : 2183
StartDateTime        : 2/2/2015 1:02:41 PM
EndDateTime          : 2/2/2015 1:02:38 PM
Duration              : -00:00:03.2300000
CreatedDateTime       : 2/2/2015 1:02:53 PM
Status               : Completed
ProtectionGroupName  : Clone
SmProtectionGroupId   : 34
PolicyName            : Vault
SmPolicyId            : 18
BackupName            : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus    : NotVerified
```

3. Restore-SmBackupコマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

MySQLのリストア処理の監視

[Job]ページを使用して、SnapCenterの各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中

-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  てリストをフィルタリングし、リストア処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*復元*を選択します。
 - d. *ステータス*ドロップダウンリストから、復元ステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. 復元ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

MySQLリソースのバックアップをクローニング

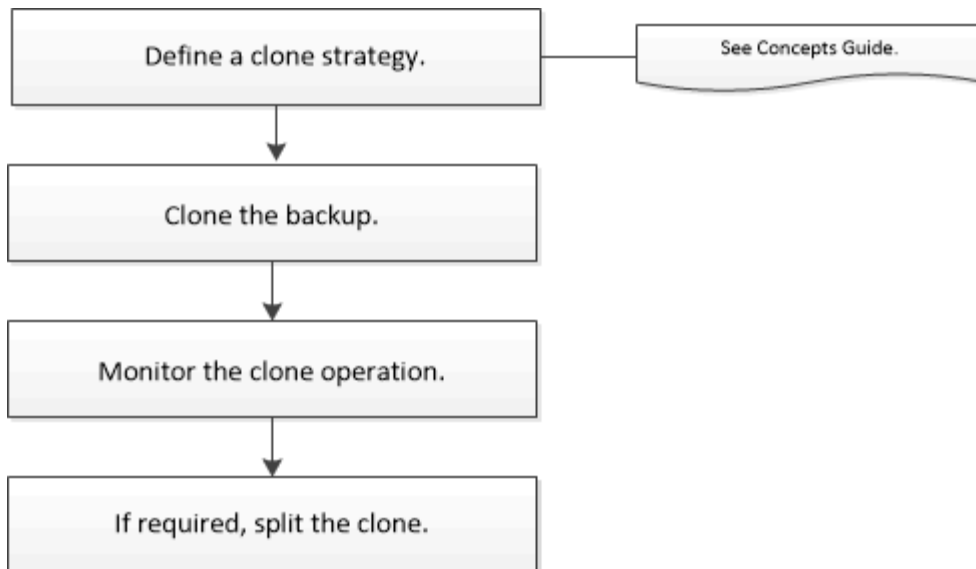
クローニングのワークフロー

クローニング ワークフローには、クローニング処理の実行と処理の監視が含まれます。

タスク概要

- ソースMySQLサーバでクローニング処理を実行できます。
- リソースのバックアップをクローニングする理由には次のものがあります。
 - アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のリソースの構造およびコンテンツを使用してテストするため
 - データの抽出と操作を行うツールで、データ ウェアハウスにデータを取り込むため
 - 誤って削除または変更されたデータをリカバリするため

次のワークフローは、クローニング処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

MySQLバックアップのクローニング

SnapCenterを使用してバックアップをクローニングすることができます。クローニングはプライマリとセカンダリのどちらのバックアップからも実行できます。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- ボリュームをホストするアグリゲートがStorage Virtual Machine (SVM) の割り当て済みアグリゲート リストに含まれていることを確認します。
- クローニング前またはクローニング後のコマンドについては、プラグイン ホストの次のパスで使用できるコマンド リストにコマンドが存在するかどうかを確認する必要があります。
 - Windows ホスト上のデフォルトの場所: `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux ホスト上のデフォルトの場所: `/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



コマンドがコマンド リストに存在しない場合、処理は失敗します。* MySQL 5.7 バージョンの場合、MySQL.properties ファイルで IGNORE_MYSQLX_PORT = true (デフォルトでは false) を設定する必要があります。

タスク概要

- クローニングされたMySQLインスタンスを保護することはできません。
- FlexCloneボリューム分割操作の詳細については、以下を参照してください。 <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["親ボリュームからのFlexCloneボリュームのスプリット"]。
- ONTAP 9.12.1 以前のバージョンでは、復元の一環としてSnapLock Vault スナップショットから作成されたクローンには、 SnapLock Vault の有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホスト、関連するリソース グループとポリシー、ステータスなどの情報とともに表示されます。

3. リソースまたはリソース グループを選択します。

リソース グループを選択した場合はリソースを選択する必要があります。

リソースまたはリソース グループのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージ システムから [バックアップ] を選択します。
5. 表からデータバックアップを選択し、クリックします。 。
6. [Location] ページで、次の操作を実行します。

フィールド	操作
Clone server	クローンをどのホスト上に作成するかを選択します。
ポート	クローニングされたMySQLインスタンスを起動するポートを指定します。
NFS Export IP Address	クローン ボリュームをエクスポートするホスト名またはIPアドレスを入力します。

7. [Scripts] ページで、次の手順を実行します。



スクリプトはプラグイン ホストで実行されます。

- a. クローニング処理の前後に実行するプリコマンドやポストコマンドを入力します。
 - クローニング前のコマンド：同じ名前の既存のデータベースの削除
 - クローニング後のコマンド：データベースの検証やデータベースの起動
- b. ホストにファイルシステムをマウントするには、mount コマンドを入力します。

Linuxマシンのボリュームまたはqtreeに対するmountコマンド：

NFSの例: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

- 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。

- 概要を確認し、[完了] をクリックします。
- モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレット

手順

- Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
PS C:\> Open-SmConnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

- Get-SmBackupコマンドレットを使用して、クローニング処理を実行するバックアップを取得します。

この例では、クローニングできるバックアップが2つあります。

```
C:\PS> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
1	Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM	

- 既存のバックアップからクローニング処理を開始し、クローニングされたボリュームをエクスポートするNFSエクスポートのIPアドレスを指定します。

この例では、NFSExportIPsのアドレスを10.32.212.14と指定してバックアップをクローニングしています。

```
PS C:\> New-SmClone -AppPluginCode MySQL -BackupName  
"scs000211748_gdl_englab_netapp_com_MySQL_mysqlld_3306_scs000211748_0  
6-26-2024_06.08.35.4307" -Resources  
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqlld_3306"}  
-Port 3320 -CloneToHost shivarhel30.rtp.openenglab.netapp.com
```




NFSExportIPsを指定しない場合、デフォルトでクローン ターゲット ホストにエクスポートされます。

4. Get-SmCloneReportコマンドレットを使用してクローニング ジョブの詳細を表示し、バックアップが正常にクローニングされたことを確認します。

クローンID、開始日時、終了日時などの詳細を確認できます。

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration             : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName           : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName     : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources       : {Don, Betty, Bobby, Sally}
ClonedResources       : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError            :
```

MySQLのクローン処理の監視

SnapCenterのクローニング処理の進捗状況を、[Jobs]ページで監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した

-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター* ページで、*ジョブ* をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  でリストをフィルタリングし、クローニング処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ* ドロップダウンリストから*クローン*を選択します。
 - d. *ステータス* ドロップダウンリストからクローンのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. クローンジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. ジョブの詳細ページで、*ログの表示* をクリックします。

クローンのスプリット

SnapCenterを使用して、クローン リソースを親リソースからスプリットできます。スプリットされたクローンは親リソースから独立します。

タスク概要

- 中間クローンではクローン スプリット処理を実行できません。

たとえば、データベース バックアップからクローン1を作成したあとで、クローン1のバックアップを作成し、そのバックアップ（クローン2）をクローニングできます。クローン2を作成すると、クローン1は中間クローンになり、クローン1ではクローン スプリット処理を実行できなくなります。ただし、クローン2に対してはクローン スプリット処理を実行できます。

クローン2をスプリットすると、クローン1は中間クローンではなくなるため、クローン1に対してクローン スプリット処理を実行できるようになります。

- クローンをスプリットすると、そのクローンのバックアップ コピーとクローン ジョブが削除されます。
- FlexCloneボリューム分割操作の詳細については、以下を参照してください。 ["親ボリュームからFlexCloneボリュームのスプリット"](#)。
- ストレージ システム上のボリュームまたはアグリゲートがオンラインであることを確認します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. *リソース* ページで、表示リストから適切なオプションを選択します。

オプション	説明
データベース アプリケーションの場合	表示リストから*データベース*を選択します。
ファイルシステムの場合	表示リストから*パス*を選択します。

3. リストから適切なリソースを選択します。

リソースのトポロジ ページが表示されます。

4. *コピーの管理*ビューから、クローンされたリソース（データベースやLUNなど）を選択し、*をクリックします。
5. 分割するクローンの推定サイズとアグリゲート上で必要な空き容量を確認し、[開始] をクリックします。
6. モニター > ジョブ をクリックして、操作の進行状況を監視します。

SMCoreサービスが再起動されると、クローン スプリット処理は応答を停止します。Stop-SmJobコマンドレットを実行してクローン スプリット処理を停止してから、クローン スプリット処理を再試行してください。

クローンが分割されているかどうかを確認するためのポーリング時間を長くしたり短くしたりする場合は、*SMCoreServiceHost.exe.config* ファイルの *CloneSplitStatusCheckPollTime* パラメータの値を変更して、SMCore がクローン分割操作のステータスをポーリングする時間間隔を設定できます。値はミリ秒単位で、デフォルト値は5分です。

例えば：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

バックアップ、リストア、または別のクローン スプリットが実行中の場合、クローン スプリットの開始処理は失敗します。クローン スプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

["アグリゲートが存在しないためにSnapCenterのクローニングや検証が失敗する"](#)

SnapCenterアップグレード後のMySQLデータベースのクローンの削除またはスプリット

SnapCenter 4.3にアップグレードすると、クローンは表示されなくなります。クローンを作成したリソースの[Topology]ページで、クローンの削除やスプリットを実行できます。

タスク概要

非表示のクローンのストレージ フットプリントを見つける場合は、次のコマンドを実行します。Get-SmClone -ListStorageFootprint

手順

1. remove-smbbackupコマンドレットを使用して、クローニングされたリソースのバックアップを削除します。
2. remove-smresourcegroupコマンドレットを使用して、クローニングされたリソースのリソース グループを削除します。
3. remove-smprotectresourceコマンドレットを使用して、クローニングされたリソースの保護を解除します。
4. [Resources]ページで親リソースを選択します。

リソースのトポロジ ページが表示されます。

5. [Manage Copies]ビューで、プライマリまたはセカンダリ（ミラー先またはレプリケート先）ストレージシステムからクローンを選択します。
6. クローンを選択し、クリックします  クローンを削除するには、または  クローンを分割します。
7. [OK]をクリックします。

NetAppがサポートするプラグインを使用してアプリケーションを保護する

NetAppがサポートしているプラグイン

NetAppがサポートしているプラグインの概要

使用するアプリケーションには、MongoDB、ORASCPM (Oracle アプリケーション)、SAP ASE、SAP MaxDB、ストレージ プラグインなどのNetApp対応プラグインを使用し、SnapCenterを使用してこれらのアプリケーションをバックアップ、復元、またはクローン化できます。NetAppがサポートしているプラグインは、NetApp SnapCenterソフトウェアのホスト側コンポーネントとして動作し、アプリケーションに対応したリソースのデータ保護と管理を提供します。

NetAppがサポートしているプラグインをインストールすると、SnapCenterとNetApp SnapMirrorテクノロジーを使用して別のボリュームのバックアップ セットのミラー コピーを作成し、NetApp SnapVaultテクノロジーを使用してディスクツーディスクのバックアップ レプリケーションを実行できます。NetAppがサポートしているプラグインは、WindowsとLinuxのどちらの環境でも使用できます。



SnapCenterCLIでは、NetAppがサポートしているプラグイン コマンドはサポートされません。

NetApp は、SnapCenterに組み込まれたプラグイン フレームワークを使用してONTAPストレージ上のデータ ボリュームのデータ保護操作を実行するためのストレージ プラグインを提供します。

NetAppでサポートされているプラグインは、「ホストの追加」 ページからインストールできます。

"ホストを追加し、リモート ホストにプラグイン パッケージをインストールします。"



SnapCenterサポート ポリシーは、プラグイン フレームワーク、コア エンジン、および関連 API のサポートをカバーします。プラグインのソース コードおよびプラグイン フレームワーク上に構築された関連スクリプトはサポートの対象外となります。

NetAppがサポートしているプラグインの機能

データ保護操作には、MongoDB、ORASCPM、Oracle Applications、SAP ASE、SAP MaxDB、ストレージ プラグインなどのNetAppがサポートするプラグインを使用できます。

- データベース、インスタンス、ドキュメント、表領域などのリソースを追加します。
- バックアップを作成します。
- バックアップからリストアします。
- バックアップをクローニングします。
- バックアップ処理のスケジュールを設定します。
- バックアップ、リストア、クローニングの各処理を監視します。

- バックアップ、リストア、クローニングの各処理のレポートを表示します。

データ保護操作には、NetAppがサポートするプラグインを使用できます。

- ONTAPクラスタ間でストレージ ボリュームの整合グループSnapshotを作成します。
- 組み込みのプレ / ポスト スクリプト フレームワークを使用して、カスタム アプリケーションをバックアップします。

ONTAPボリューム、LUN、またはqtreeをバックアップできます。

- SnapCenterポリシーを使用して、既存のレプリケーション関係（SnapVault / SnapMirror / ユニファイドレプリケーション）を利用して、プライマリで作成されたSnapshotをONTAPセカンダリに更新します。

ONTAPプライマリおよびセカンダリには、ONTAP FAS、AFF、ASA、ONTAP Select、またはCloud Volumes ONTAP を使用できます。

- ONTAPボリューム、LUN、またはファイル全体をリカバリします。

ブラウズ機能またはインデックス機能が製品に組み込まれていないため、それぞれのファイル パスを手動で指定する必要があります。

qtreeまたはディレクトリのリストアはサポートされていませんが、バックアップ範囲がqtreeレベルで定義されている場合は、qtreeに限りクローニングとエクスポートを実行できます。

NetAppがサポートしているプラグインの特長

SnapCenterは、プラグイン アプリケーションと統合されるほか、ストレージ システム上でNetAppの数々のテクノロジーと統合されます。MongoDB、ORASCPM (Oracle アプリケーション)、SAP ASE、SAP MaxDB、ストレージ プラグインなどのNetApp対応プラグインを操作するには、SnapCenterグラフィカル ユーザー インターフェイスを使用します。

- 統合されたグラフィカルユーザーインターフェース

SnapCenterのインターフェイスは、すべてのプラグインと環境で標準化され、一貫しています。どのプラグインでも、SnapCenterのインターフェイスから、バックアップ、リストア、リカバリ、クローニングの各処理を一貫した方法で実行できるほか、ダッシュボード ビューで概要を把握したり、ロールベース アクセス制御（RBAC）を設定したり、ジョブを監視したりすることができます。

- 自動化された中央管理

バックアップ処理のスケジュールを設定したり、ポリシーベースのバックアップ保持を設定したり、リストア処理を実行したりできます。SnapCenterからのEメール アラートの送信を設定して、環境をプロアクティブに監視することもできます。

- 無停止の**NetApp**スナップショットテクノロジー

SnapCenterでは、NetAppがサポートしているプラグインでNetApp Snapshotテクノロジーを使用してリソースがバックアップされます。Snapshotはストレージ スペースを最小限しか消費しません。

NetAppがサポートするプラグインには、次のような利点もあります。

- バックアップ、リストア、およびクローニングのワークフローがサポートされます。
- セキュリティがRBACでサポートされ、ロール委譲が一元化されます。

クレデンシャルを設定して、許可されたSnapCenterユーザにアプリケーションレベルのアクセス権を付与することもできます。

- NetApp FlexCloneテクノロジーを使用して、テストまたはデータ抽出に使用するリソースのコピー（スペース効率に優れたポイントインタイム コピー）を作成できます。

クローンを作成するストレージ システムにFlexCloneライセンスが必要です。

- バックアップの作成でONTAPの整合グループ（CG）のSnapshot機能がサポートされます。
- 複数のリソース ホストで同時に複数のバックアップを実行できます。

1回の処理で、1つのホストの複数のリソースが同じボリュームを共有する場合に複数のSnapshotが統合されます。

- 外部コマンドを使用してSnapshotを作成できます。
- Windows環境でファイルシステムと整合性のあるSnapshotを作成できます。

NetAppがサポートしているプラグインでサポートされるストレージ タイプ

SnapCenterは、物理マシンと仮想マシンの両方でさまざまなストレージ タイプをサポートしています。NetAppがサポートしているプラグインをインストールする前に、ストレージ タイプがサポートされているかどうかを確認する必要があります。

マシン	ストレージ タイプ
VMホストへの物理およびNFSの直接マウント（VMDKとRDM LUNはサポートされていません）。	FC接続LUN
VMホストへの物理およびNFSの直接マウント（VMDKとRDM LUNはサポートされていません）。	iSCSI接続LUN
VMホストへの物理およびNFSの直接マウント（VMDKとRDM LUNはサポートされていません）。	NFS接続ボリューム
VMware ESXi	NFSとSANの両方に存在するvVolデータストア vVolデータストアは、ONTAP Tools for VMware vSphereでのみプロビジョニングできます。

NetAppがサポートしているプラグインに必要な最小ONTAP権限

必要な最小ONTAP権限は、データ保護に使用するSnapCenterプラグインによって異なる

ります。

- 全アクセス コマンド: ONTAP 9.12.1 以降に必要な最小限の権限
 - event generate-autosupport-log
 - job history show
 - job stop
 - lun attribute show
 - lun create
 - lun delete
 - lun geometry
 - lun igroup add
 - lun igroup create
 - lun igroup delete
 - lun igroup rename
 - lun igroup show
 - lun mapping add-reporting-nodes
 - lun mapping create
 - lun mapping delete
 - lun mapping remove-reporting-nodes
 - lun mapping show
 - lun modify
 - lun move-in-volume
 - lun offline
 - lun online
 - lun resize
 - lun serial
 - lun show
 - ネットワークインターフェース
 - snapmirror policy add-rule
 - snapmirror policy modify-rule
 - snapmirror policy remove-rule
 - snapmirror policy show
 - snapmirror restore
 - snapmirror show
 - snapmirror show-history
 - snapmirror update
 - snapmirror update-ls-set
 - snapmirror list-destinations

- version
- volume clone create
- volume clone show
- volume clone split start
- volume clone split stop
- volume create
- volume destroy
- volume file clone create
- volume file show-disk-usage
- volume offline
- volume online
- volume modify
- volume qtree create
- volume qtree delete
- volume qtree modify
- volume qtree show
- volume restrict
- volume show
- volume snapshot create
- volume snapshot delete
- volume snapshot modify
- volume snapshot rename
- volume snapshot restore
- volume snapshot restore-file
- volume snapshot show
- volume unmount
- vservers cifs
- vservers cifs share create
- vservers cifs share delete
- vservers cifs shadowcopy show
- vservers cifs share show
- vservers cifs show
- vservers export-policy create
- vservers export-policy delete
- vservers export-policy rule create
- vservers export-policy rule show
- vservers export-policy show

- vservers iscsi connection show
- vservers show
- 読み取り専用コマンド: ONTAP 8.3.0以降に必要な最小限の権限
 - ネットワークインターフェース

NetAppがサポートしているプラグインでSnapMirrorおよびSnapVaultレプリケーションを使うためのストレージ システムの準備

SnapCenterプラグインと一緒にONTAP SnapMirrorテクノロジーを使用すると、バックアップ セットのミラー コピーを別のボリュームに作成できます。また、ONTAP SnapVaultを使用すれば、標準への準拠やその他のガバナンスを目的としたディスクツリー ディスクのバックアップ レプリケーションを実行できます。これらのタスクを実行する前に、ソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、その関係を初期化する必要があります。

SnapCenterは、Snapshot処理の完了後に、SnapMirrorとSnapVaultに対する更新を実行します。SnapMirror更新とSnapVault更新は、SnapCenterジョブの一部として実行されるため、ONTAPスケジュールを別途作成しないでください。



NetApp SnapManager製品からSnapCenterに移行した場合、データ保護関係が適切に設定されていれば、このセクションは省略してかまいません。

データ保護関係では、プライマリ ストレージ（ソース ボリューム）上のデータがセカンダリ ストレージ（デスティネーション ボリューム）にレプリケートされます。この関係を初期化すると、ソース ボリュームで参照されるデータ ブロックがデスティネーション ボリュームに転送されます。



SnapCenter は、 SnapMirrorとSnapVaultボリューム間のカスケード関係をサポートしていません (* プライマリ * > ミラー > ボールト)。ファンアウト関係を使用する必要があります。

SnapCenterは、バージョンに依存しないSnapMirror関係の管理をサポートしています。バージョンに依存しないSnapMirror関係とその設定方法の詳細については、["ONTAPのドキュメント"](#)。

バックアップ戦略の定義

バックアップ ジョブを作成する前にバックアップ戦略を定義しておく、リソースの正常なリストアやクローニングに必要なバックアップを確実に作成できます。バックアップ戦略の大部分は、サービス レベル アグリーメント（SLA）、目標復旧時間（RTO）、および目標復旧時点（RPO）によって決まります。

タスク概要

SLAとは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。RTOは、サービスの停止からビジネス プロセスの復旧までに必要となる時間です。RPOは、障害発生後に通常処理を再開するためにバックアップ ストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLA、RTO、およびRPOは、データ保護戦略に関与します。

手順

1. リソースをバックアップするタイミングを決定します。
2. 必要なバックアップ ジョブの数を決定します。
3. バックアップの命名方法を決定します。
4. 整合グループSnapshotを保持するかどうかを決定し、保持する場合は整合グループSnapshotを削除する適切なオプションを決定します。
5. レプリケーションのためにNetApp SnapMirrorテクノロジーを使用するか、または長期保持のためにNetApp SnapVaultテクノロジーを使用するかを決定します。
6. ソース ストレージ システムおよびSnapMirrorデスティネーションでのSnapshotの保持期間を確認します。
7. バックアップ処理の前後にコマンドを実行するかどうかを決定し、実行する場合はプリスクリプトまたはポストスクリプトを用意します。

NetAppがサポートしているプラグインのバックアップ戦略

NetAppがサポートしているプラグイン リソースのバックアップ スケジュール

バックアップのスケジュールを決定する場合に最も重要な要因となるのは、リソースの変更率です。リソースをバックアップする回数が多いほど、リストア時にSnapCenterが使用する必要のあるアーカイブ ログの数が少なくなります。これにより、リストア処理の時間を短縮できます。

使用頻度の高いリソースは1時間ごとにバックアップする必要がありますが、ほとんど使用されないリソースは1日に1回バックアップすれば十分です。その他の要因としては、組織におけるリソースの重要性、サービス レベル アグリーメント（SLA）、目標復旧時点（RPO）などがあります。

SLAとは、求められるサービス レベル、およびサービスに関連する多くの問題（サービスの可用性やパフォーマンスなど）への対応を定義したものです。RPOは、障害発生後に通常処理を再開するためにバックアップ ストレージからリカバリする必要があるファイルの経過時間に関する戦略を定義したものです。SLAとRPOは、データ保護戦略に関与します。

バックアップ スケジュールには、次の2つの要素があります。

- バックアップ頻度

バックアップ頻度（バックアップを実行する間隔）は、ポリシー設定の一部であり、一部のプラグインではスケジュール タイプとも呼ばれます。たとえば、毎時、毎日、毎週、または毎月としてバックアップ頻度を設定できます。SnapCenter GUI で [設定] > [ポリシー] をクリックすると、ポリシーにアクセスできます。

- バックアップ スケジュール

バックアップ スケジュール（バックアップが実行される日時）は、リソースまたはリソース グループの設定の一部です。たとえば、週次バックアップのポリシーが設定されているリソース グループがある場合、毎週木曜日の午後 10 時にバックアップするようにスケジュールを設定できます。SnapCenter GUI でリソース グループのスケジュールにアクセスするには、[リソース] をクリックし、適切なプラグインを選択して、[表示] > [リソース グループ] をクリックします。

必要なバックアップ ジョブの数

必要なバックアップ ジョブの数を左右する要因としては、リソースのサイズ、使用中のボリュームの数、リソースの変更率、サービス レベル アグリーメント (SLA) などがあります。

通常、選択するバックアップ ジョブの数は、リソースが配置されているボリュームの数に応じて決まります。たとえば、あるボリュームに小規模なリソースのグループを配置しており、別のボリュームに1つの大規模なリソースを配置している場合は、小規模なリソース用のバックアップ ジョブと大規模なリソース用のバックアップ ジョブを1つずつ作成できます。

手動で追加したNetAppがサポートしているプラグイン リソースでサポートされるリストア戦略のタイプ

SnapCenterを使用してリストア処理を正常に実行するには、戦略を定義しておく必要があります。手動で追加したNetAppがサポートしているプラグイン リソースのリストア戦略には、2つのタイプがあります。



手動で追加したNetAppがサポートしているプラグイン リソースはリカバリできません。

リソース全体のリストア

- リソースのすべてのボリューム、qtree、およびLUNをリストア



リソースにボリュームまたはqtreeが含まれている場合、そのボリュームまたはqtreeのリストア用のSnapshotが選択されたあとに作成されたSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。

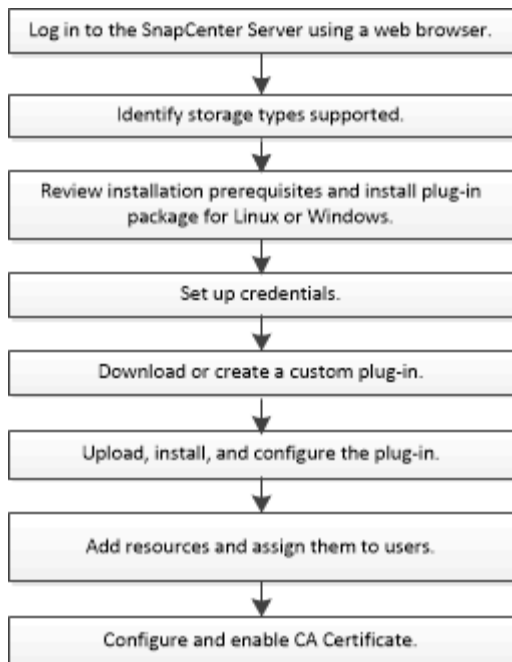
ファイルレベルのリストア

- ボリューム、qtree、またはディレクトリからファイルをリストア
- 選択したLUNのみをリストア

NetAppがサポートしているプラグインのインストール準備

SnapCenter NetAppがサポートしているプラグインのインストール ワークフロー

NetAppがサポートしているプラグイン リソースを保護する場合は、NetAppがサポートしているSnapCenterプラグインをインストールしてセットアップする必要があります。



Windows、Linux、または AIX 用のホストを追加し、プラグイン パッケージをインストールするための前提条件

ホストを追加してプラグイン パッケージをインストールする前に、すべての要件を満たしておく必要があります。NetAppがサポートするプラグインは、Windows、Linux、および AIX 環境でサポートされます。

 ストレージおよび Oracle アプリケーションは AIX でサポートされます。

- Linux、Windows、または AIX ホストに Java 11 がインストールされている必要があります。

 IBM Java は Windows および Linux ホストではサポートされていません。

- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。
- MongoDB、ORASCPM、Oracle Applications、SAP ASE、SAP MaxDB、ストレージ プラグインなどのNetAppでサポートされているプラグインは、ホスト追加操作が実行されるクライアント ホストで使用できる必要があります。

全般

iSCSIを使用している場合は、iSCSIサービスが実行されている必要があります。

Windowsホスト

- ローカル管理者権限があり、リモート ホストに対してローカル ログインのアクセス許可があるドメイン ユーザが必要です。
- SnapCenterでクラスタ ノードを管理する場合は、クラスタ内のすべてのノードに対する管理者権限があるユーザが必要です。

- Microsoft Windows 用のSnapCenterプラグインを手動で選択する必要があります。

["Windows用JAVAをダウンロード"](#)

LinuxおよびAIXホスト



ストレージおよび Oracle アプリケーションは AIX でサポートされます。

- rootユーザまたはroot以外のユーザに対してパスワード ベースのSSH接続を有効にしておく必要があります。
- Java 11をLinuxホストにインストールしておく必要があります。

SnapCenter ServerホストにWindows Server 2019またはWindows Server 2016を使用している場合は、Java 11をインストールする必要があります。要件に関する最新の情報については、Interoperability Matrix Tool (IMT) を参照してください。

["Linux用JAVAをダウンロード"](#)

["AIX用JAVAをダウンロード"](#)

["NetApp Interoperability Matrix Tool"](#)

- いくつかのパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。visudo Linuxユーティリティを使用して、/etc/sudoersファイルに次の行を追加します。



Sudoバージョン1.8.7以降を使用していることを確認します。

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

LINUX_USER は、作成した非 root ユーザーの名前です。

checksum_value は、次の場所にある **sc_unix_plugins_checksum.txt** ファイルから取得できます。

- SnapCenter Server が Windows ホストにインストールされている場合は、`C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`。
- SnapCenter Server が Linux ホストにインストールされている場合は、`/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`。



この例は、独自のデータを作成する際の参照としてのみ使用してください。

AIXホストの要件

SnapCenter Plug-ins Package for AIXをインストールする前に、ホストが要件を満たしていることを確認する必要があります。



ストレージおよび Oracle アプリケーションは AIX でサポートされます。



SnapCenter Plug-ins Package for AIXに含まれているSnapCenter Plug-in for UNIXでは、同時ボリューム グループはサポートされません。

項目	要件
オペレーティング システム	AIX 7.1以降
ホスト上のSnapCenterプラグインに必要な最小RAM	4 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	2 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	Java 11 IBM Java Javaを最新バージョンにアップグレードした場合は、 <code>/var/opt/snapcenter/spl/etc/spl.properties</code> にあるJAVA_HOMEオプションが正しいJavaバージョンと正しいパスに設定されていることを確認する必要があります。

サポートされているバージョンに関する最新情報については、["NetApp Interoperability Matrix Tool"](#)。

AIXホストのroot以外のユーザへのsudo権限の設定

SnapCenter 4.4以降では、root以外のユーザがSnapCenter Plug-ins Package for AIXをインストールしてログイン プロセスを開始できます。プラグイン プロセスは有効なroot以外のユーザとして実行されます。いくつかのパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

必要なもの

- sudoバージョン1.8.7以降
- /etc/ssh/sshd_config ファイルを編集して、メッセージ認証コード アルゴリズム (MAC hmac-sha2-256 および MAC hmac-sha2-512) を設定します。

この構成ファイルを更新したら、sshdサービスを再起動します。

例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

このタスクについて

次のパスにアクセスできるようにroot以外のユーザにsudo権限を設定する必要があります。

- /home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /custom_location/NetApp/snapcenter/spl/installation/plugins/uninstall
- /custom_location/NetApp/snapcenter/spl/bin/spl

手順

1. SnapCenter Plug-ins Package for AIXをインストールするAIXホストにログインします。
2. visudo Linuxユーティリティを使用して、/etc/sudoersファイルに次の行を追加します。


```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



RAC をセットアップしている場合は、他の許可されたコマンドとともに、`/etc/sudoers` ファイルに次の行を追加する必要があります: `'/<crs_home>/bin/olsnodes'`

`crs_home` の値は、`/etc/oracle/olr.loc` ファイルから取得できます。

`AIX_USER` は、作成した非 root ユーザーの名前です。

`checksum_value` は、次の場所にある `sc_unix_plugins_checksum.txt` ファイルから取得できます。

- SnapCenter Server が Windows ホストにインストールされている場合は、`C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`。
- SnapCenter Server が Linux ホストにインストールされている場合は、`/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt`。



この例は、独自のデータを作成する際の参照としてのみ使用してください。

SnapCenter Plug-ins Package for Windowsをインストールするホストの要件

SnapCenter Plug-ins Package for Windowsをインストールする前に、ホスト システムのスペースとサイジングに関する基本的な要件を理解しておく必要があります。

項目	要件
オペレーティング システム	Microsoft Windows サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。

項目	要件
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	5 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	• ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドル • PowerShell Core 7.4.2 • Java 11 Oracle JavaおよびOpenJDK Java 11 Oracle Java および OpenJDK は、SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp対応プラグイン、および Windows ホストにインストールできるその他のカスタム アプリケーションにのみ必要です。 サポートされているバージョンに関する最新情報については、"NetApp Interoperability Matrix Tool"。

LinuxおよびAIX用のSnapCenterプラグインパッケージをインストールするためのホスト要件

Linux または AIX 用のSnapCenterプラグイン パッケージをインストールする前に、ホストが要件を満たしていることを確認する必要があります。



ストレージおよび Oracle アプリケーションは AIX でサポートされます。

項目	要件
オペレーティング システム	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
ホスト上のSnapCenterプラグインに必要な最小RAM	1 GB

項目	要件
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	2 GB  十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。
必要なソフトウェア パッケージ	Java 11 Oracle JavaまたはOpenJDK Javaを最新バージョンにアップグレードした場合は、/var/opt/snapcenter/spl/etc/spl.propertiesにあるJAVA_HOMEオプションが正しいJavaバージョンと正しいパスに設定されていることを確認する必要があります。

サポートされているバージョンに関する最新情報については、 ["NetApp Interoperability Matrix Tool"](#)

NetAppがサポートしているプラグインのクレデンシャルの設定

SnapCenterは、クレデンシャルを使用してSnapCenterの処理を実行するユーザを認証します。SnapCenterプラグインのインストールに使用するクレデンシャルと、データベースやWindowsファイルシステムでのデータ保護処理に使用するクレデンシャルをそれぞれ作成する必要があります。

開始する前に

- LinuxまたはAIXホスト

Linux または AIX ホストにプラグインをインストールするための資格情報を設定する必要があります。

このクレデンシャルは、rootユーザ、またはプラグインをインストールしてプロセスを開始するsudo権限があるroot以外のユーザに対して設定します。

ベスト プラクティス: ホストをデプロイしてプラグインをインストールした後でも Linux の認証情報を作成できますが、ベスト プラクティスとしては、SVM を追加した後、ホストをデプロイしてプラグインをインストールする前に認証情報を作成します。

- Windowsホスト

プラグインのインストール前にWindowsクレデンシャルを設定する必要があります。

このクレデンシャルには、管理者権限（リモート ホストに対する管理者権限を含む）を設定する必要があります。

- NetAppがサポートしているプラグイン アプリケーション

プラグインは、選択または作成されたクレデンシャルをリソースの追加時に使用します。データ保護操作中にリソースが資格情報を必要としない場合は、資格情報を なし に設定できます。

タスク概要

個々のリソース グループのクレデンシャルを設定する場合で、ユーザ名に完全なadmin権限が割り当てられていない場合は、少なくともリソース グループとバックアップの権限を割り当てる必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[資格情報]をクリックします。
3. *新規*をクリックします。
4. *資格情報*ページで、資格情報の設定に必要な情報を指定します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。
ユーザ名	認証に使用するユーザ名とパスワードを入力します。 • ドメイン管理者または管理者グループの任意のメンバー ドメイン管理者またはSnapCenterプラグインをインストールするシステムの管理者グループの任意のメンバーを指定します。ユーザ名フィールドの有効な形式は次のとおりです。 ◦ <i>NetBIOS</i>\ユーザー名 ◦ ドメイン<i>FQDN</i>\ユーザー名 • ローカル管理者（ワークグループの場合のみ） ワークグループに属するシステムの場合は、SnapCenterプラグインをインストールするシステムに組み込みのローカル管理者を指定します。ユーザ アカウントに昇格された権限がある場合、またはホスト システムでユーザ アクセス制御機能が無効になっている場合は、ローカル管理者グループに属するローカル ユーザ アカウントを指定できます。ユーザー名フィールドの有効な形式は次のとおりです: <i>UserName</i>
パスワード	認証に使用するパスワードを入力します。
Authentication Type	使用する認証タイプを選択します。

フィールド	操作
Use sudo privileges	非 root ユーザーの資格情報を作成する場合は、[sudo 権限を使用する] チェックボックスをオンにします。  Linux および AIX ユーザーのみに適用されます。

5. [OK]をクリックします。

クレデンシャルの設定が完了したら、必要に応じて[User and Access]ページでユーザやユーザ グループにクレデンシャルを割り当てることができます。

Windows Server 2016以降でのgMSAの設定

Windows Server 2016以降では、作成したグループ管理サービス アカウント (gMSA) を通じて、管理対象ドメイン アカウントからサービス アカウントのパスワードを自動管理できます。

開始する前に

- Windows Server 2016以降のドメイン コントローラが必要です。
- ドメインのメンバーであるWindows Server 2016以降のホストが必要です。

手順

1. KDSルート キーを作成し、gMSA内のオブジェクトごとに一意のパスワードを生成します。
2. 各ドメインについて、Windowsドメインコントローラから次のコマンドを実行します: Add-KDSRootKey -EffectiveImmediately
3. gMSAを作成して設定します。
 - a. 次の形式でユーザ グループ アカウントを作成します。

```
domainName\accountName$
.. コンピュータ オブジェクトをグループに追加します。
.. 作成したユーザ グループを使用してgMSAを作成します。
```

次に例を示します。

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. 走る `Get-ADServiceAccount` サービス アカウントを確認するコマンド。
```

4. ホストでgMSAを設定します。

- a. gMSAアカウントを使用するホストで、Windows PowerShell用のActive Directoryモジュールを有効にします。

これを行うには、PowerShellから次のコマンドを実行します。

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. ホストを再起動します。
 - b. PowerShell コマンド プロンプトから次のコマンドを実行して、ホストに gMSA をインストールします。 `Install-AdServiceAccount <gMSA>`
 - c. 次のコマンドを実行して、gMSA アカウントを確認します。 `Test-AdServiceAccount <gMSA>`
5. ホスト上の設定済みgMSAに管理者権限を割り当てます。
 6. SnapCenter Serverで設定済みのgMSAアカウントを指定してWindowsホストを追加します。

SnapCenter Serverにより、選択したプラグインがホストにインストールされ、プラグインのインストール時には指定したgMSAがサービスのログオン アカウントとして使用されます。

NetAppがサポートしているプラグインのインストール

ホストの追加とリモート ホストへのプラグイン パッケージのインストール

ホストを追加するには、SnapCenter のホストの追加ページを使用し、プラグイン パッケージをインストールする必要があります。プラグインは、自動的にリモート ホストにインストールされます。ホストの追加とプラグイン パッケージのインストールは、ホストごとまたはクラスタごとに実行できます。

開始する前に

- この操作は、SnapCenter Adminロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。

- メッセージ キュー サービスが実行中であることを確認する必要があります。
- グループ管理サービス アカウント (gMSA) を使用する場合は、管理者権限でgMSAを設定する必要があります。

"Windows Server 2016以降でカスタム アプリケーションのグループ管理サービス アカウントを設定する"

- Windows ホストの場合は、必ず Windows 用SnapCenterプラグインを選択する必要があります。

タスク概要

- SnapCenter Serverをプラグイン ホストとして別のSnapCenter Serverに追加することはできません。
- クラスタ (WSFC) にプラグインをインストールする場合、プラグインはクラスタのすべてのノードにインストールされます。

手順

1. 左側のナビゲーション ペインで、[ホスト] を選択します。
2. 上部の*管理対象ホスト*タブが選択されていることを確認します。
3. *追加*を選択します。
4. [Hosts]ページで、次の操作を実行します。

フィールド	操作
ホストタイプ	ホスト タイプを選択します。 • Windows • Linux • AIX  NetAppがサポートするプラグインは、Windows、Linux、AIX 環境で使用できます。  ストレージおよび Oracle アプリケーションは AIX でサポートされます。

フィールド	操作
ホスト名	ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。 SnapCenterが機能するためには、DNSが適切に設定されている必要があります。そのため、FQDNを入力することを推奨します。 Windows環境の場合、信頼されないドメイン ホストのIPアドレスがサポートされるのは、そのIPアドレスがFQDNに解決される場合のみです。 スタンドアロン ホストのIPアドレスまたはFQDNを入力できます。 SnapCenterを使用してサブドメインの一部であるホストを追加する場合は、FQDNを指定する必要があります。
Credentials	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモート ホストに対する管理権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 指定したクレデンシャル名にカーソルを合わせると、クレデンシャルの詳細を確認できます。  クレデンシャルの認証モードは、[Add Host]ウィザードで指定するホスト タイプによって決まります。

5. *インストールするプラグインの選択*セクションで、インストールするプラグインを選択します。

リストから次のプラグインをインストールできます。

- MongoDB
- ORASCPM（Oracle Applicationsとして表示）
- SAP ASE
- SAP MaxDB
- ストレージ

6. (オプション) 他のプラグインをインストールするには、[その他のオプション] を選択します。

フィールド	操作
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。 デフォルトのポート番号は8145です。SnapCenter Serverがカスタム ポートにインストールされている場合は、そのポート番号がデフォルト ポートとして表示されます。  プラグインを手動でインストールしてカスタム ポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理が失敗します。
Installation Path	NetAppがサポートするプラグインは、Windows システムまたは Linux システムのいずれかにインストールできます。 - Windows 用のSnapCenterプラグイン パッケージの場合、デフォルトのパスは C:\Program Files\ NetApp\ SnapCenterです。 必要に応じて、パスをカスタマイズできます。 - Linux用SnapCenterプラグインパッケージおよびAIX用SnapCenterプラグインパッケージの場合、デフォルトのパスは /opt/NetApp/snapcenter。 必要に応じて、パスをカスタマイズできます。
Skip preinstall checks	プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスをオンにします。

フィールド	操作
Use group Managed Service Account (gMSA) to run the plug-in services	Windowsホストで、グループ管理サービス アカウ ント（gMSA）を使用してプラグイン サービスを実 行する場合は、このチェック ボックスをオンにし ます。  gMSA名 をdomainName\accountName\$の形 式で指定します。  gMSAは、SnapCenter Plug-in for Windowsサービスのログオン サービ ス アカウントとしてのみ使用されま す。

7. *送信*を選択します。

「事前チェックをスキップ」チェックボックスを選択していない場合、ホストがプラグインのインストール要件を満たしているかどうかを確認するための検証が行われます。ディスク容量、RAM、PowerShellバージョン、.NETバージョン、場所（Windowsプラグインの場合）、Javaバージョン（Linuxプラグインの場合）が最小要件に照らして検証されます。最小要件を満たしていない場合、対応するエラーまたは警告メッセージが表示されます。

エラーがディスク容量またはRAMに関連している場合は、次の場所にあるweb.configファイルを更新できます。`C:\Program Files\NetApp\SnapCenter WebApp`デフォルト値を変更します。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。



HA セットアップでSnapManager.Web.UI.dll.config を更新する場合は、両方のノードでファイルを更新し、 SnapCenterアプリケーション プールを再起動する必要があります。

Windowsのデフォルトパスは C:\Program Files\NetApp\SnapCenter
WebApp\SnapManager.Web.UI.dll.config

Linuxのデフォルトパスは

/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config

8. ホスト タイプが Linux の場合は、フィンガープリントを確認し、[確認して送信] を選択します。



前述の手順で同じホストがSnapCenterに追加され、フィンガープリントが確認された場合でも、フィンガープリントの検証は必須です。

9. インストールの進捗状況を監視します。

インストール固有のログファイルは次の場所にあります。`/custom\_location/snapcenter/`ログ。

コマンドレットを使用して、**Linux**、**Windows**、または **AIX** 用の**SnapCenter**プラグイン パッケージを複数のリモート ホストにインストールします。

Install-SmHostPackage PowerShell コマンドレットを使用して、Linux、Windows、または AIX 用の**SnapCenter**プラグイン パッケージを複数のホストに同時にインストールできます。

開始する前に

ホストを追加するユーザには、ホストに対する管理権限が必要です。



ストレージおよび Oracle アプリケーションは AIX でサポートされます。

手順

1. PowerShellを起動します。
2. SnapCenter Serverホストで、Open-SmConnectionコマンドレットを使用してセッションを確立し、クレデンシャルを入力します。
3. Install-SmHostPackageコマンドレットと必要なパラメータを使用して、複数のホストにプラグインをインストールします。

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、-skipprecheckオプションを使用できます。

4. リモート インストールのクレデンシャルを入力します。

コマンドライン インターフェイスを使用した**Linux**ホストへの**NetApp**がサポートしているプラグインのインストール

NetAppがサポートしているプラグインは、SnapCenterユーザ インターフェイス (UI) を使用してインストールする必要があります。SnapCenter UIからのプラグインのリモート インストールが許可されていない環境では、コマンドライン インターフェイス (CLI) を使用して、コンソール モードまたはサイレント モードでNetAppがサポートしているプラグインをインストールできます。

手順

1. C:\ProgramData\NetApp\SnapCenter\Package RepositoryにあるSnapCenter Plug-ins Package for Linuxのインストール ファイル (snapcenter_linux_host_plugin.bin) を、NetAppがサポートしているプラグインのインストール先ホストにコピーします。

このパスには、SnapCenter Serverがインストールされているホストからアクセスできます。

2. コマンド プロンプトから、インストール ファイルをコピーしたディレクトリに移動します。
3. プラグインをインストールします。

```
path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address  
-DSERVER_HTTPS_PORT=port_number_for_server
```

- -DPORT は SMCORE HTTPS 通信ポートを指定します。
- -DSERVER_IP は、 SnapCenter Server の IP アドレスを指定します。
- -DSERVER_HTTPS_PORT は、 SnapCenter Server の HTTPS ポートを指定します。
- -DUSER_INSTALL_DIR は、Linux 用のSnapCenterプラグイン パッケージをインストールするディレクトリを指定します。
- _DINSTALL_LOG_NAME はログ ファイルの名前を指定します。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. Add-Smhostコマンドレットと必要なパラメータを使用して、SnapCenter Serverにホストを追加します。

コマンドで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

5. SnapCenterにログインし、UIまたはPowerShellコマンドレットを使用して、NetAppがサポートしているプラグインをアップロードします。

NetAppがサポートするプラグインは、UIからアップロードできます。"[ホストの追加とリモート ホストへのプラグイン パッケージのインストール](#)"セクション。

PowerShellコマンドレットの詳細については、SnapCenterのコマンドレットのヘルプを使用するか、コマンドレットのリファレンス情報を参照してください。

"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

NetAppがサポートしているプラグインのインストール ステータスの監視

[Jobs]ページを使用して、SnapCenterプラグイン パッケージのインストールの進捗状況を監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、プラグインのインストール操作のみがリストされるようにリストをフィルタリングするには、次の手順を実行します。
 - a. *フィルター*をクリックします。
 - b. オプション：開始日と終了日を指定します。
 - c. [タイプ] ドロップダウン メニューから、[プラグインのインストール] を選択します。
 - d. [Status]ドロップダウン メニューから、インストールのステータスを選択します。
 - e. *適用*をクリックします。
4. インストール ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

CA証明書の設定

CA証明書CSRファイルの生成

証明書署名要求（CSR）を生成し、生成したCSRを使用して認証局（CA）から取得した証明書をインポートできます。証明書には秘密キーが関連付けられます。

CSRはエンコードされたテキストのブロックであり、署名済みCA証明書を取得するために認定証明書ベンダーに提供されます。



CA 証明書の RSA キーの長さは最低 3072 ビットである必要があります。

CSRを生成するための情報については、["CA証明書CSRファイルの生成方法"](#)。



ドメイン (*.domain.company.com) またはシステム (machine1.domain.company.com) の CA 証明書を所有している場合は、CA 証明書 CSR ファイルの生成をスキップできます。SnapCenterを使用して、既存のCA証明書を導入できます。

クラスタ構成の場合、クラスタ名（仮想クラスタFQDN）と、それぞれのホスト名がCA証明書に記載されている必要があります。証明書を取得する前に、サブジェクト別名 (SAN) フィールドに入力することで証明書を更新できます。ワイルドカード証明書 (*.domain.company.com) の場合、証明書にはドメインのすべてのホスト名が暗黙的に含まれます。

CA証明書のインポート

Microsoft管理コンソール（MMC）を使用して、SnapCenter ServerとWindowsホスト プラグインにCA証明書をインポートする必要があります。

手順

1. Microsoft 管理コンソール (MMC) に移動し、[ファイル] > [スナップインの追加と削除] をクリックします。

2. [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
3. 証明書スナップイン ウィンドウで、[コンピューター アカウント] オプションを選択し、[完了] をクリックします。
4. コンソール ルート > 証明書 - ローカル コンピューター > 信頼されたルート証明機関 > 証明書 をクリックします。
5. 「信頼されたルート証明機関」フォルダを右クリックし、[すべてのタスク] > [インポート] を選択して、インポート ウィザードを起動します。
6. 次の手順でウィザードを実行します。

ウィザード ウィンドウ	操作
秘密キーのインポート	*はい*オプションを選択し、秘密キーをインポートして、*次へ*をクリックします。
インポート ファイル形式	変更せずに、[次へ] をクリックします。
セキュリティ	エクスポートされた証明書に使用する新しいパスワードを指定し、[次へ] をクリックします。
証明書のインポート ウィザードの完了	概要を確認し、[完了] をクリックしてインポートを開始します。



インポートする証明書は秘密キーとバンドルされている必要があります (サポートされている形式は **.pfx**、**.p12**、および ***.p7b** です)。

7. 「個人用」フォルダに対して手順5を繰り返します。

CA証明書のサムプリントの取得

証明書サムプリントは、証明書を識別するための16進数の文字列です。サムプリントは、サムプリント アルゴリズムを使用して証明書の内容から計算されます。

手順

1. GUIで次の手順を実行します。
 - a. 証明書をダブルクリックします。
 - b. [証明書] ダイアログボックスで、[詳細] タブをクリックします。
 - c. フィールドのリストをスクロールして、「拇印」をクリックします。
 - d. ボックスから16進数の文字をコピーします。
 - e. 16進数の間のスペースを削除します。

たとえば、拇印が「a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b」の場合、スペースを削除すると「a909502dd82ae41433e6f83886b00d4277a32a7b」になります。

2. PowerShellで、次の手順を実行します。

- a. 次のコマンドを実行して、インストールされている証明書のサムプリントを表示し、最近インストールされた証明書をサブジェクト名で識別します。

```
Get-ChildItem -Path 証明書:\LocalMachine\My
```

- b. サムプリントをコピーします。

Windowsホスト プラグイン サービスでのCA証明書の設定

インストールされているデジタル証明書をアクティブ化するには、Windowsホスト プラグイン サービスを使用してCA証明書を設定する必要があります。

SnapCenter Serverと、CA証明書がすでに導入されているすべてのプラグイン ホストで、次の手順を実行します。

手順

1. 次のコマンドを実行して、既存の証明書とSMCoreのデフォルト ポート8145とのバインドを削除します。

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例えば：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

． 次のコマンドを実行して、新しくインストールした証明書をWindowsホスト プラグイン サービスとバインドします。

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例えば：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

LinuxホストでのNetAppがサポートしているプラグイン サービスのCA証明書の設定

インストールされたデジタル証明書をアクティブ化するには、 SnapCenterプラグイン サービスを使用して、プラグイン キーストアとその証明書のパスワードを管理し、CA 証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成 し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、`/opt/NetApp/snapcenter/scc/etc`にあるファイル「keystore.jks」を使用します。

プラグインキーストアのパスワードと使用中のCA署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

キー「KEYSTORE_PASS」に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```

・ キーストア内の秘密キー
エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

`agent.properties` ファイルのキー KEYSTORE_PASS も同様に更新します。

3. パスワードを変更したら、サービスを再起動します。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは同じである必要があります。

ルート証明書または中間証明書をプラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグイン キーストアが含まれるフォルダーに移動します: `/opt/NetApp/snapcenter/scc/etc`。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. ルート証明書か中間証明書を追加します。

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

・ ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアにCA署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグイン キーストア /opt/ NetApp/snapcenter/scc/etc が含まれるフォルダーに移動します。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

6. キーストアに追加された新しいCA証明書に対応するエイリアスが、キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのプラグイン キーストア パスワードは、agent.properties ファイルのキー KEYSTORE_PASS の値です。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

・ CA 証明書のエイリアス名が長く、スペースや特殊文字（「*」、「」）が含まれている場合は、エイリアス名を単純な名前に変更します。

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

・ agent.properties ファイルのCA証明書からエイリアス名を設定します。

この値を、キーSCC_CERTIFICATE_ALIASに対して更新します。

8. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

プラグインの証明書失効リスト（CRL）を構成する

タスク概要

- ・ SnapCenterプラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。

- SnapCenterプラグインの CRL ファイルのデフォルト ディレクトリは、「opt/NetApp/snapcenter/scc/etc/crl」です。

手順

1. キーCRL_PATHに対して、agent.propertiesファイルのデフォルト ディレクトリを変更、更新できます。

このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

WindowsホストでのNetAppがサポートしているプラグイン サービスのCA証明書の設定

インストールされたデジタル証明書をアクティブ化するには、SnapCenterプラグインサービスを使用して、プラグイン キーストアとその証明書のパスワードを管理し、CA証明書を構成し、プラグイン トラストストアにルート証明書または中間証明書を構成し、プラグイン トラストストアに CA 署名キー ペアを構成する必要があります。

プラグインは、信頼ストアとキーストアの両方として、C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etcにあるファイル *keystore.jks* を使用します。

プラグインキーストアのパスワードと使用中の**CA**署名キーペアのエイリアスを管理する

手順

1. プラグイン エージェント プロパティ ファイルからプラグイン キーストアのデフォルト パスワードを取得できます。

これはキー_KEYSTORE_PASS_に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```



Windowsコマンド プロンプトで「keytool」 コマンドが認識されない場合は、keytoolコマンドを完全なパスに置き換えます。

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe" -storepasswd -keystore keystore.jks
```

3. キーストア内の秘密キー エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

```
keytool -keypasswd -alias "証明書内のエイリアス名" -keystore keystore.jks
```

agent.properties ファイルのキー KEYSTORE_PASS も同様に更新します。

4. パスワードを変更したら、サービスを再起動します。



プラグイン キーストアのパスワードと、秘密キーに関連付けられたすべてのエイリアス パスワードは同じである必要があります。

ルート証明書または中間証明書をプラグイン信頼ストアに設定する

信頼ストアをプラグインするには、秘密キーなしでルート証明書または中間証明書を構成する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `_C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_` に移動します。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. ルート証明書か中間証明書を追加します。

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. ルート証明書または中間証明書をプラグイン信頼ストアに設定した後、サービスを再起動します。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

プラグイン信頼ストアに**CA**署名キーペアを構成する

CA 署名キー ペアをプラグイン信頼ストアに設定する必要があります。

手順

1. プラグインキーストアが格納されているフォルダ `_C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc_` に移動します。
2. ファイル `keystore.jks` を見つけます。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

4. 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

6. キーストアに追加された新しいCA証明書に対応するエイリアスが、キーストアに含まれていることを確認します。
7. CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

デフォルトのプラグイン キーストア パスワードは、`agent.properties` ファイルのキー `KEYSTORE_PASS` の値です。

```
keytool -keypasswd -alias "CA証明書のエイリアス名" -keystore keystore.jks
```

8. *agent.properties* ファイル内の CA 証明書からエイリアス名を設定します。

この値を、キー `SCC_CERTIFICATE_ALIAS` に対して更新します。

9. CA 署名キー ペアをプラグイン トラスト ストアに設定した後、サービスを再起動します。

SnapCenterプラグインの証明書失効リスト (CRL) を構成する

タスク概要

- 関連するCA証明書の最新のCRLファイルをダウンロードするには、"[SnapCenter CA証明書の証明書失効リストファイルを更新する方法](#)"。
- SnapCenterプラグインは、事前に構成されたディレクトリ内の CRL ファイルを検索します。
- SnapCenterプラグインの CRL ファイルのデフォルト ディレクトリは、'`C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\ etc\crl`' です。

手順

1. キー `CRL_PATH` に対して、*agent.properties* ファイル内のデフォルト ディレクトリを変更および更新できます。
2. このディレクトリには、複数のCRLファイルを格納できます。

受信する証明書については、それぞれのCRLに対して検証が行われます。

プラグインのCA証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインでCA証明書の検証を有効にする必要があります。

開始する前に

- 実行 `Set-SmCertificateSettings` コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- `Get-SmCertificateSettings` を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで使用するパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. プラグイン ホストを1つまたは複数選択します。
4. *その他のオプション*をクリックします。
5. *証明書の検証を有効にする*を選択します。

終了後の操作

[Managed Hosts]タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Serverとプラグイン ホスト間の接続のステータスを示します。

- *  * は、CA 証明書が有効になっていないか、プラグイン ホストに割り当てられていないことを示します。
- *  * は CA 証明書が正常に検証されたことを示します。
- *  * は、CA 証明書を検証できなかったことを示します。
- *  * は接続情報を取得できなかったことを示します。



ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

データ保護の準備

NetAppがサポートしているプラグインを使用するための前提条件

ユーザがSnapCenter NetAppがサポートしているプラグインを使用するために、SnapCenter管理者が事前にSnapCenter Serverをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter Serverをインストールして設定します。
- SnapCenter Serverにログインします。
- SnapCenter環境を設定するために、必要に応じて、ストレージ システム接続を追加し、クレデンシャルを作成します。
- ホストを追加し、プラグインをインストールしてアップロードします。
- 必要に応じて、Java 11をプラグインのホストにインストールします。
- データ パス (LIF) が複数ある場合、またはdNFS構成を使用している場合は、データベース ホストでSnapCenter CLIを使用して次の作業を実行できます。
 - デフォルトでは、データベース ホストのすべての IP アドレスが、クローン ボリュームのストレージ 仮想マシン (SVM) の NFS ストレージ エクスポート ポリシーに追加されます。IPアドレスを1つにするか、一部のIPアドレスに制限する場合は、Set-PreferredHostIPsInStorageExportPolicy CLIを実行します。
 - SVM に複数のデータ パス (LIF) がある場合、SnapCenter はNFS クローン ボリュームをマウントするための適切なデータ パス (LIF) を選択します。ただし、データ パス (LIF) を1つに特定する場合は、Set-SvmPreferredDataPath CLIを実行する必要があります。コマンドで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、["SnapCenterソフトウェア コマンド リファレンス ガイド"](#)。
- バックアップ レプリケーションが必要である場合は、SnapMirrorとSnapVaultをセットアップします。
- ポート9090がホストの他のアプリケーションで使用されていないことを確認します。

SnapCenterで必要な他のポートに加え、ポート9090をNetAppがサポートしているプラグイン用に確保しておく必要があります。

NetAppがサポートしているプラグイン リソースの保護におけるリソース、リソース グループ、ポリシーの使用法

SnapCenterを使用する前に、実行するバックアップ、クローニング、リストアの各処理

に関連する基本的な概念を理解しておく役立ちます。ここでは、これらの処理で扱うリソース、リソース グループ、およびポリシーについて説明します。

- リソースとは、SnapCenterでバックアップやクローンを作成するデータベース、Windowsファイルシステム、VMなどです。
- SnapCenterリソース グループは、ホストまたはクラスタ上のリソースの集まりです。

リソース グループに対して処理を実行すると、リソース グループに指定したスケジュールに従って、リソース グループに定義されているリソースに対して処理が実行されます。

単一のリソースまたはリソース グループをオンデマンドでバックアップすることができます。また、スケジュールされたバックアップを単一リソースおよびリソース グループに対して実行することもできます。

- ポリシーは、バックアップ頻度、コピーの保持、レプリケーション、スクリプトといった、データ保護処理の特性を指定するものです。

リソース グループを作成するときに、そのグループに対して1つ以上のポリシーを選択します。単一リソースに対してオンデマンドでバックアップを実行するときにもポリシーを選択できます。

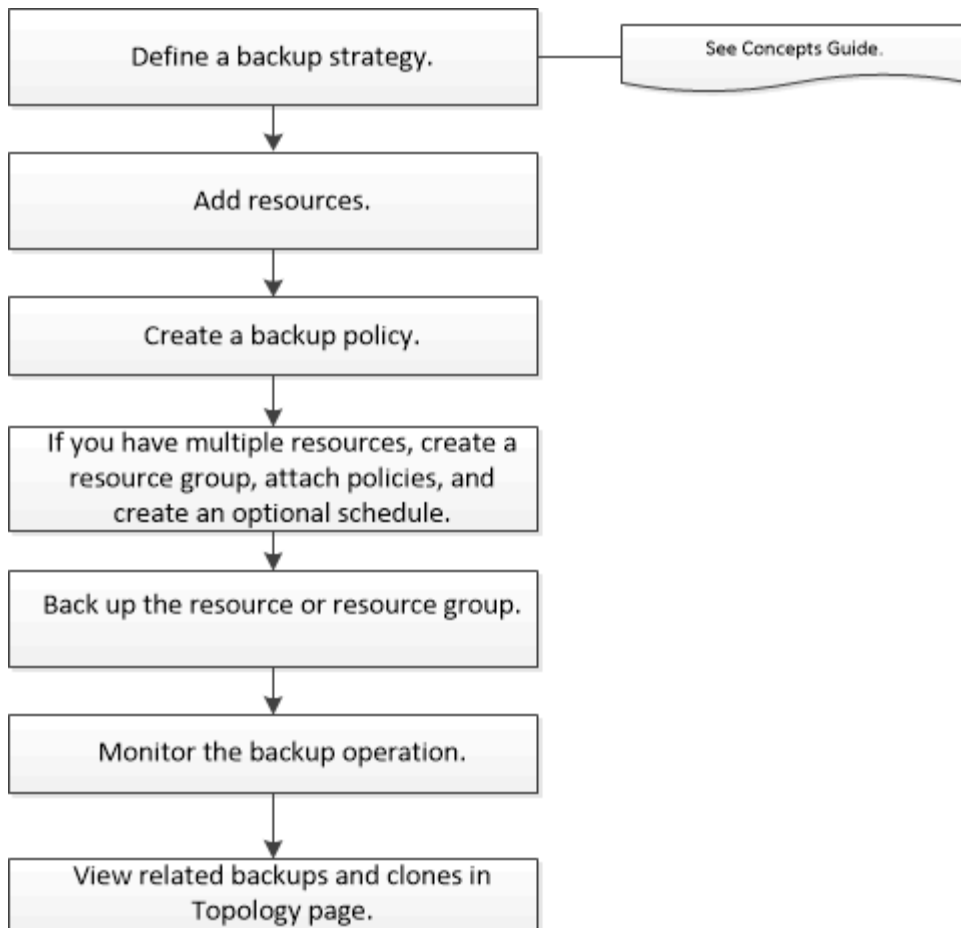
リソース グループは、保護する対象と、それを日時でいつ保護するかを定義するものと考えてください。ポリシーとは、それをどのように保護したいかを定義するものと考えてください。たとえば、すべてのデータベースまたはホストのすべてのファイルシステムをバックアップする場合、すべてのデータベースまたはホストのすべてのファイルシステムを含むリソース グループを作成します。このリソース グループに、日次ポリシーと毎時ポリシーの2つのポリシーを適用します。リソース グループを作成してポリシーを適用する際に、ファイルベースのバックアップを1日1回実行するようにリソース グループを設定し、別のスケジュールでSnapshotベースのバックアップを1時間おきに実行するように設定します。

NetAppがサポートしているプラグイン リソースのバックアップ

NetAppがサポートしているプラグイン リソースのバックアップ

バックアップのワークフローには、計画、バックアップするリソースの特定、バックアップ ポリシーの管理、リソース グループの作成とポリシーの適用、バックアップの作成、処理の監視が含まれます。

次のワークフローは、バックアップ処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、[SnapCenterコマンドレットのヘルプ](#)を使用するか、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"

NetAppがサポートしているプラグインへのリソースの追加

バックアップまたはクローンを作成するリソースを追加する必要があります。環境によっては、バックアップまたはクローンを作成するデータベース インスタンスやそのコレクションもリソースに含まれます。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の作成、クレデンシャルの追加などのタスクを完了しておく必要があります。
- SnapCenter Serverにプラグインをアップロードしておく必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[リソースの追加] を選択します。
3. [Provide Resource Details] ページで、次の操作を実行します。

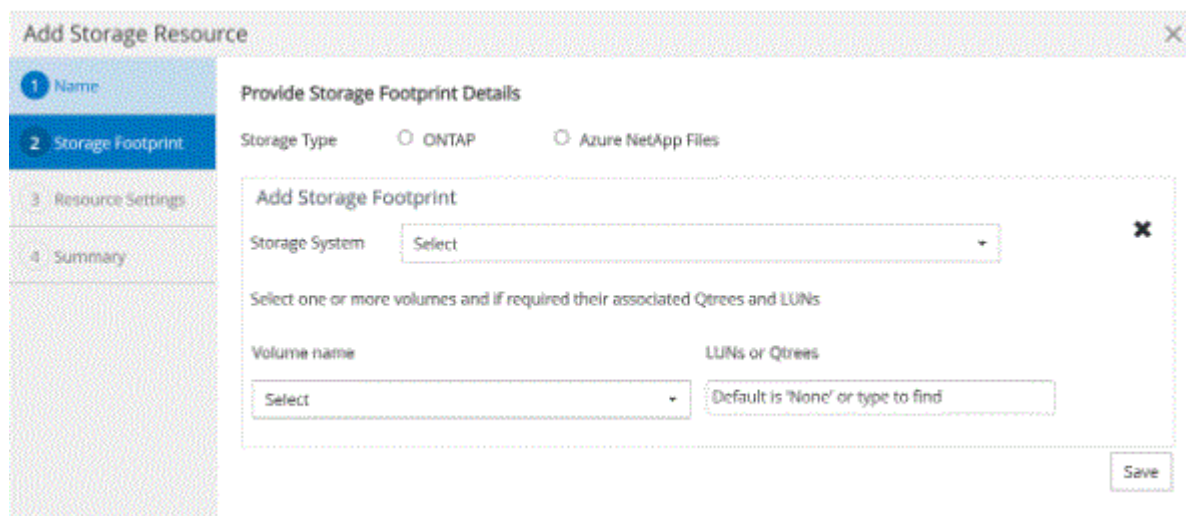
フィールド	操作
Name	リソースの名前を入力します。
ホスト名	ホストを選択します。
タイプ	タイプを選択します。タイプは、プラグイン定義ファイルにあるユーザ定義のタイプです。たとえば、データベースやインスタンスなどになります。 選択したタイプに親がある場合は、親の詳細を入力します。たとえば、タイプがデータベースでその親がインスタンスの場合、インスタンスの詳細を入力します。
資格情報名	クレデンシャルを選択するか、新しいクレデンシャルを作成します。
Mount Paths	リソースのマウント先のマウントパスを入力します。これは、Windowsホストにのみ適用されます。

4. [ストレージ フットプリントの提供] ページで、ストレージ システムを選択し、1 つ以上のボリューム、LUN、および qtree を選択して、[保存] を選択します。

オプション:  アイコンをクリックして、他のストレージ システムからボリューム、LUN、qtree を追加します。



NetAppがサポートしているプラグインでは、リソースの自動検出はサポートされていません。物理環境と仮想環境のストレージの詳細も自動検出されません。リソースの作成時に、物理環境と仮想環境のストレージの情報を指定する必要があります。



5. [Resource Settings] ページで、リソースのカスタムのキーと値のペアを指定します。



カスタム キー名が大文字であることを確認します。

Resource settings ⓘ

Custom key-value pairs for MySQL plug-in

Name	Value	
HOST	localhost	✕
PORT	3306	✕
MASTER_SLAVE	NO	+ ✕

それぞれのプラグインパラメータについては、"[リソースを設定するためのパラメータ](#)"

6. 概要を確認し、[完了] を選択します。

結果

リソースは、タイプ、ホストまたはクラスタ名、関連するリソース グループとポリシー、全体的なステータスなどの情報とともに表示されます。



SnapCenterの外部でデータベースの名前が変更された場合は、リソースを更新する必要があります。

終了後の操作

アセットへのアクセスを他のユーザに許可する場合は、SnapCenter管理者が対象のユーザにアセットを割り当てる必要があります。これにより、ユーザは、自身に割り当てられたアセットに対して、権限のある処理を実行できるようになります。

リソースを追加したあとで、リソースの詳細を変更できます。NetAppがサポートしているプラグイン リソースにバックアップが関連付けられている場合、リソース名、リソース タイプ、およびホスト名のフィールドを変更することはできません。

リソースを設定するためのパラメータ

プラグインを手動で追加する場合は、[Resource Settings] ページで次のパラメータを使用してリソースを設定できます。

Plug-in for MongoDB

Resource Settings :

- MongoDB_APP_SERVER= (リソース タイプが共有クラスタの場合) または MongoDB_ReplicaSet_SERVER= (リソース タイプがレプリカセットの場合)
- OPLOG_PATH= (MongoDB.propertiesfileから指定する場合はオプション パラメータ)
- MONGODB_AUTHENTICATION_TYPE= (LDAP認証の場合はPLAIN、それ以外の場合はNone)

MongoDB.propertiesファイルには、次のパラメータを指定する必要があります。

- DISABLE_STARTING_STOPPING_SERVICES=

- N：プラグインによってサービスの開始と停止が実行される場合。
- サービスの開始/停止がユーザーによって実行される場合はY。
- オプション パラメータのデフォルト値はNに設定されています。
- OPLOG_PATH_ = (SnapCenterでカスタムのキーと値のペアとしてすでに提供されている場合のオプションのパラメーター)。

Plug-in for MaxDB

Resource Settings :

- XUSER_ENABLE (Y|N)は、データベース ユーザがパスワードを要求されないように、MaxDBでxuserの使用を有効または無効にします。
- HANDLE_LOGWRITER (Y|N)は、ログライターの一時停止 (N) またはログライターの再開 (Y) の処理を実行します。
- DBMCLICMD (path_to_dbmcli_cmd)は、MaxDB dbmcliコマンドへのパスを指定します。設定されていない場合は、検索パスでdbmcliが使用されます。



Windows環境では、パスを二重引用符 ("...") で囲む必要があります。

- SQLCLICMD (path_to_sqlcli_cmd)は、MaxDB sqlcliコマンドへのパスを指定します。パスが設定されていない場合は、検索パスでsqlcliが使用されます。
- MaxDB_UPDATE_HIST_LOG (Y|N)は、MaxDB履歴ログを更新するかどうかを、MaxDBバックアップ プログラムに指示します。
- MAXDB_CHECK_SNAPSHOT_DIR: 例、SID1:directory[,directory...]; [SID2:directoary[,directory...]] は、Snap Creator スナップショット コピー操作が成功したことを確認し、スナップショットが作成されたことを確認します。

これはNFSにのみ該当します。ディレクトリは、.snapshotディレクトリが格納されている場所を指している必要があります。複数のディレクトリをカンマで区切って指定できます。

MaxDB 7.8以降のバージョンでは、データベースのバックアップ要求はバックアップ履歴でFailedとマークされます。

- MAXDB_BACKUP_TEMPLATES: 各データベースのバックアップ テンプレートを指定します。

テンプレートが存在し、外部タイプのバックアップ テンプレートである必要があります。MaxDB 7.8以降でSnapshot統合を有効にするには、MaxDBバックグラウンド サーバ機能があり、外部タイプのMaxDBバックアップ テンプレートがすでに設定されている必要があります。

- MAXDB_BG_SERVER_PREFIX: バックグラウンド サーバー名のプレフィックスを指定します。

MAXDB_BACKUP_TEMPLATESパラメータが設定されている場合は、MaxDB_BG_SERVER_PREFIXパラメータも設定する必要があります。プレフィックスを設定しない場合は、デフォルト値 na_bg_ が使用されます。

SAP ASE 用プラグイン

Resource Settings :

- SYBASE_SERVER (data_server_name) には、Sybaseデータ サーバ名を指定します (isqlコマンドの-S オプション)。たとえば、p_testのように指定します。
- SYBASE_DATABASES_EXCLUDE (db_name) では、「all」要素を使用するとデータベースを除外できます。

複数のデータベースを指定するには、セミコロンで区切ったリストを使用します。例：pubs2;test_db1。

- SYBASE_USER: user_nameには、isqlコマンドを実行できるオペレーティング システム ユーザを指定します。

UNIXの場合は必須です。このパラメータは、Snap Creator Agentのstartコマンドとstopコマンドを実行するユーザ（通常はrootユーザ）とisqlコマンドを実行するユーザが異なる場合に必須です。

- SYBASE_TRAN_DUMP db_name:directory_pathは、Snapshotの作成後にSybaseトランザクション ダンプを実行できるようにします。例：pubs2:/sybasedumps/ pubs2

トランザクション ダンプが必要な各データベースを指定する必要があります。

- Sybase_Tran_dump_compress (Y|N)は、Sybaseトランザクション ダンプのネイティブ圧縮を有効または無効にします。
- Sybase_ISQL_CMD (例：/opt/Sybase/OCS-15_0/bin/isql) は、isqlコマンドへのパスを定義します。
- SYBASE_EXCLUDE_TEMPDB (Y|N)を使用すると、ユーザが作成した一時データベースを自動的に除外できます。

Plug-in for Oracle Applications (ORASCPM)

Resource Settings :

- SQLPLUS_CMDには、SQLplusへのパスを指定します。
- ORACLE_DATABASESは、バックアップするOracleデータベースと対応するユーザ (database:user) を一覧表示します。
- CNTL_FILE_BACKUP_DIRには、制御ファイルのバックアップ先ディレクトリを指定します。
- ORA_TEMPには、一時ファイルのディレクトリを指定します。
- ORACLE_HOMEには、Oracleソフトウェアがインストールされているディレクトリを指定します。
- ARCHIVE_LOG_ONLYには、アーカイブ ログをバックアップするかどうかを指定します。
- ORACLE_BACKUPMODE は、オンライン バックアップを実行するかオフライン バックアップを実行するかを指定します。
- ORACLE_EXPORT_PARAMETERS は、/bin/su <sqlplus を実行しているユーザー> -c sqlplus /nolog <cmd> の実行中に、上記で定義された環境変数を再エクスポートするかどうかを指定します。これは通常、sqlplus を実行しているユーザーが、connect / as sysdba を使用してデータベースに接続するために必要なすべての環境変数を設定していない場合に発生します。

NetAppがサポートしているプラグイン リソースのポリシーの作成

SnapCenterを使用してNetAppがサポートしているプラグイン固有のリソースをバックアップする前に、バックアップ対象のリソースまたはリソース グループのバックアップポリシーを作成する必要があります。

開始する前に

- バックアップ戦略を定義しておく必要があります。

詳細については、NetAppがサポートしているプラグインのデータ保護戦略の定義に関する説明を参照してください。

- データ保護の準備が完了している必要があります。

データ保護の準備作業には、SnapCenterのインストール、ホストの追加、ストレージ システム接続の作成、リソースの追加などがあります。

- ミラー処理またはバックアップ処理を実行するには、Storage Virtual Machine (SVM) をユーザに割り当てる必要があります。

ユーザがSnapshotをミラーまたはバックアップにレプリケートする場合は、ソース ボリュームとデスティネーション ボリューム両方のSVMをSnapCenter管理者がユーザに割り当てる必要があります。

- 保護するリソースを手動で追加しておく必要があります。

タスク概要

- バックアップ ポリシーとは、バックアップをどのように管理し、スケジューリングし、保持するかを定める一連のルールです。レプリケーション、スクリプト、アプリケーション設定を指定することもできます。
- ポリシーでオプションを指定しておくことで、別のリソース グループにポリシーを再利用して時間を節約することができます。
- SnapLock
 - [Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで指定した保持日数以下にする必要があります。
 - Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、ポリシーで指定した数よりも多くのSnapshotが保持される可能性があります。
 - ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。



プライマリSnapLock設定はSnapCenterバックアップ ポリシーで管理し、セカンダリSnapLock設定はONTAPで管理します。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[ポリシー]をクリックします。
3. *新規*をクリックします。
4. 「名前」 ページで、ポリシー名と詳細を入力します。
5. [Policy type]ページで、次の手順を実行します。
 - a. ストレージ タイプを選択します。
 - b. カスタム バックアップ設定セクションでは、キーと値の形式でプラグインに渡す必要がある特定のバックアップ設定を指定します。

プラグインに渡すキーと値のペアを複数指定することができます。

6. スナップショットとレプリケーション ページで、次の手順を実行します。

- a. オンデマンド、時間別、日次、週次、または*月次*を選択してスケジュール タイプを指定します。



リソース グループを作成する際に、バックアップ処理のスケジュール（開始日、終了日、頻度）を指定することができます。これにより、ポリシーとバックアップ間隔が同じである複数のリソース グループを作成できますが、各ポリシーに異なるバックアップ スケジュールを割り当てることもできます。



午前 2 時にスケジュールを設定した場合、夏時間 (DST) 中はスケジュールは実行されません。

- a. スナップショット設定セクションで、バックアップ タイプ ページで選択したバックアップ タイプとスケジュール タイプの保持設定を指定します。

状況	操作
特定の数のSnapshotを保持	*保持するコピー*を選択し、保持するスナップショットの数を指定します。 Snapshotの数が指定した数を超えると、古いものから順にSnapshotが削除されます。  SnapVaultレプリケーションを有効にする場合は、保持数を2以上に設定する必要があります。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。  最大保持値は 1018 です。保持数を、使用しているONTAPバージョンがサポートする値よりも大きい値に設定すると、バックアップが失敗します。
Snapshotを特定の日数だけ保持	*コピーの保持期間*を選択し、スナップショットを削除する前に保持する日数を指定します。
スナップショットコピーのロック期間	スナップショット コピーのロック期間 を選択し、日、月、または年を指定します。 SnapLock保持期間は100年未満にする必要があります。

b. ポリシーラベルを選択します。



リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしないでも実行できます。

7. [セカンダリ レプリケーション オプションの選択] セクションで、次のセカンダリ レプリケーション オプションの 1 つまたは両方を選択します。

フィールド	操作
ローカル スナップショット コピーを作成した後、 SnapMirror を更新します	別のボリュームにバックアップ セットのミラー コピーを作成する場合 (SnapMirrorレプリケーション) は、このフィールドを選択します。 ONTAPの保護関係のタイプがミラーとバックアップの場合、このオプションのみを選択すると、プライマリで作成されたSnapshotがデスティネーションに転送されませんが、デスティネーションのリストに表示されます。このスナップショットを復元操作を実行するために宛先から選択すると、次のエラー メッセージが表示されます: 選択したボールド/ミラー バックアップにはセカンダリ ロケーションは使用できません。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。 トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 見る "[Topology ページでのNetAppがサポートしているプラグイン リソースに関連するバックアップとクローンの表示]"。

フィールド	操作
ローカルスナップショットコピーを作成した後、 SnapVault を更新します	ディスクツーディスクのバックアップ レプリケーション (SnapVaultバックアップ) を実行する場合は、このオプションを選択します。 セカンダリ レプリケーションのSnapLockの有効期限には、プライマリSnapLockの有効期限がロードされます。トポロジ ページの 更新 ボタンをクリックすると、ONTAPから取得されたセカンダリおよびプライマリSnapLock の有効期限が更新されます。 SnapLock がSnapLock Vault と呼ばれるONTAPのセカンダリにのみ設定されている場合、[トポロジ] ページの [更新] ボタンをクリックすると、ONTAPから取得されたセカンダリのロック期間が更新されます。 SnapLock Vault の詳細については、「Vault の保存先でスナップショットを WORM にコミットする」を参照してください。 見る"TopologyページでのNetAppがサポートしているプラグイン リソースに関連するバックアップとクローンの表示"]。
エラー再試行回数	処理が停止されるまでに試行できるレプリケーションの最大回数を入力します。



セカンダリ ストレージでSnapshotの上限に達しないように、ONTAPでセカンダリ ストレージのSnapMirror保持ポリシーを設定する必要があります。

8. 概要を確認し、[完了] をクリックします。

リソース グループの作成とポリシーの適用

リソース グループはコンテナであり、バックアップして保護するリソースをここに追加する必要があります。これを使用することで、特定のアプリケーションに関連するすべてのデータを同時にバックアップできます。リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義することも必要です。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [Resources] ページで、[New Resource Group]を選択します。
3. [Name] ページで、次の操作を実行します。

フィールド	操作
Name	リソース グループの名前を入力します。 注意: リソース グループ名は 250 文字を超えてはなりません。
Tags	リソース グループを検索しやすくするために、ラベルを入力します。 たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。
Use custom name format for Snapshot copy	Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。 たとえば、 <i>customtext_resource group_policy_hostname</i> または <i>resource group_hostname</i> です。デフォルトでは、Snapshot の名前の後ろにタイムスタンプが付加されます。

4. オプション: [リソース] ページで、[ホスト] ドロップダウン リストからホスト名を選択し、[リソース タイプ] ドロップダウン リストからリソース タイプを選択します。

画面の情報がフィルタリングされます。

5. *利用可能なリソース*セクションからリソースを選択し、右矢印を選択してそれらを*選択したリソース*セクションに移動します。
6. オプション: アプリケーション設定 ページで、次の操作を行います。

- a. [Backups]の矢印を選択して、追加のバックアップ オプションを設定します。

整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for Consistency Group Snapshot operation to complete	Snapshot処理が完了するまでの待機時間として、[Urgent]、[Medium]、または[Relaxed]のいずれかを選択します。 [Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

+

- a. [Scripts]の矢印を選択し、休止、Snapshot、および休止解除の処理を行うプリコマンドとポストコマンドを入力します。障害の発生時に終了前に実行するプリコマンドも入力できます。
- b. [Custom Configurations]の矢印を選択し、このリソースを使用するすべてのデータ保護処理に必要なカスタムのキーと値のペアを入力します。

パラメータ	設定	説明
ARCHIVE_LOG_ENABLE	(Y / N)	アーカイブ ログ管理を有効にし、アーカイブ ログを削除します。
ARCHIVE_LOG_RETENTION	number_of_days	アーカイブ ログを保持する日数を指定します。 この設定は、NTAP_SNAPSHOT_RETENTIONS 以上である必要があります。
ARCHIVE_LOG_DIR	change_info_directory/logs	アーカイブ ログが含まれるディレクトリへのパスを指定します。
ARCHIVE_LOG_EXT	file_extension	アーカイブ ログ ファイルの拡張子の長さを指定します。 たとえば、アーカイブ ログが log_backup_0_0_0_0.161518551942 9 で、file_extension 値が 5 の場合、ログの拡張子は 5 桁、つまり 16151 になります。

パラメータ	設定	説明
ARCHIVE_LOG_RECURSIVE_SE ARCH	(Y / N)	サブディレクトリ内のアーカイブ ログの管理を有効にします。 アーカイブ ログがサブディレクトリの下にある場合は、このパラメータを使用する必要があります。

- c. スナップショット コピー ツール 矢印を選択して、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する（このオプションはLinux リソースには適用されません）	ファイル システムの一貫性を備えたSnapCenter * を選択します。 このオプションは、SnapCenter Plug-in for SAP HANA Databaseには適用されません。
SnapCenterでストレージ レベルのSnapshotを作成する	ファイル システムの整合性のないSnapCenter * を選択します。
Snapshotを作成するためにホストで実行するコマンドを入力する	*その他*を選択し、スナップショットを作成するためにホスト上で実行するコマンドを入力します。

7. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



を選択してポリシーを作成することもできます 。

ポリシーは、「選択したポリシーのスケジュールを構成する」セクションにリストされます。

- b. スケジュールの設定*列で*を選択します 設定するポリシーの。
- c. ポリシー *policy_name* のスケジュールの追加 ダイアログ ボックスで、スケジュールを構成し、[OK] を選択します。

*policy_name*は、選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. *通知*ページの*電子メール設定*ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP サーバーは、設定 > グローバル設定 で設定する必要があります。

9. 概要を確認し、[完了] を選択します。

リソース グループを作成し、**ASA r2** システム上のリソースの二次保護を有効にします。

ASA r2 システム上にあるリソースを追加するには、リソース グループを作成する必要があります。リソース グループの作成時にセカンダリ保護をプロビジョニングすることもできます。

開始する前に

- ONTAP 9.x リソースとASA r2 リソースの両方を同じリソース グループに追加していないことを確認する必要があります。
- ONTAP 9.x リソースとASA r2 リソースの両方を含むデータベースが存在しないことを確認する必要があります。

タスク概要

- 二次保護は、ログインしたユーザーに **SecondaryProtection** 機能が有効になっているロールが割り当てられている場合にのみ使用できます。
- セカンダリ保護を有効にすると、プライマリおよびセカンダリ整合性グループの作成中にリソース グループはメンテナンス モードになります。プライマリおよびセカンダリのコンシステンシー グループが作成されると、リソース グループのメンテナンス モードが解除されます。
- SnapCenter はクローン リソースの二次保護をサポートしていません。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。
 - a. [Name] フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag] フィールドに1つ以上のラベルを入力します。

たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

- c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- d. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。



必要に応じて、プレフィックスを含め、アプリケーションで設定されたのとまったく同じ宛先を使用する必要があります。

4. [リソース] ページで、[ホスト] ドロップダウン リストからデータベース ホスト名を選択します。



[Available Resources] セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで [Available Resources] のリストには表示されません。

5. [使用可能なリソース] セクションから ASA r2 リソースを選択し、[選択したリソース] セクションに移動します。
6. アプリケーション設定ページで、バックアップ オプションを選択します。
7. [Policies] ページで、次の手順を実行します。
 - a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックし  でポリシーを作成することもできます。

[Configure schedules for selected policies] セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの [Configure Schedules] 列で、 をクリックします。
 - c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが [Applied Schedules] 列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenter のバックアップ スケジュールと重複している場合、サポートされません。

8. 選択したポリシーに対して二次保護が有効になっている場合は、「二次保護」ページが表示されるので、次の手順を実行する必要があります。
 - a. レプリケーション ポリシーのタイプを選択します。



同期レプリケーション ポリシーはサポートされていません。

- b. 使用する整合性グループのサフィックスを指定します。
 - c. [宛先クラスタ] および [宛先 SVM] ドロップダウンから、使用するピア クラスタと SVM を選択します。



クラスタと SVM のピアリングは SnapCenter ではサポートされていません。クラスタと SVM のピアリングを実行するには、System Manager または ONTAP CLI を使用する必要があります。



リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは [セカンダリ保護リソース] セクションに表示されます。

1. [Verification]ページで、次の手順を実行します。

- a. ロケーターのロード をクリックして、 SnapMirrorまたはSnapVaultボリュームをロードし、セカンダリストレージで検証を実行します。
- b. クリック  ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で をクリックします。
- c. [Add Verification Schedules policy_name]ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

- d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証]を選択します。
- e. [OK]をクリックします。

設定した検証スケジュールが、[Applied Schedules]列にリストされます。

2. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtptServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

3. 概要を確認し、[完了] をクリックします。

PowerShellコマンドレットを使用したストレージ システム接続とクレデンシャルの作成

PowerShellコマンドレットを使用してデータ保護処理を実行するには、Storage Virtual Machine (SVM) 接続とクレデンシャルを作成しておく必要があります。

開始する前に

- PowerShellコマンドレットを実行できるようにPowerShell環境を準備しておく必要があります。
- ストレージ接続を作成するには、Infrastructure Adminロールの権限が必要です。
- プラグインのインストールが実行中でないことを確認してください。

ストレージ システム接続の追加中は、ホスト プラグインのインストールが進行中であってはなりません。ホスト キャッシュが更新されず、SnapCenter GUI にデータベースのステータスが「バックアップに使用できません」または「NetAppストレージ上にありません」と表示される可能性があるためです。

- ストレージ システムの名前は一意である必要があります。

SnapCenterでは、別々のクラスタに属している場合でも、複数のストレージ システムに同じ名前を付けることはサポートされません。SnapCenterでサポートする各ストレージ システムには、一意な名前と管理LIFの一意なIPアドレスが必要です。

手順

1. Open-SmConnectionコマンドレットを使用して、PowerShell Core接続セッションを開始します。

PowerShellセッションを開く例を次に示します。

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

2. Add-SmStorageConnectionコマンドレットを使用して、ストレージ システムへの新しい接続を作成します。

新しいストレージ システム接続を作成する例を次に示します。

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. Add-SmCredentialコマンドレットを使用して、新しいクレデンシャルを作成します。

Windowsクレデンシャルを使用してFinanceAdminという名前の新しいクレデンシャルを作成する例を次に示します。

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

NetAppがサポートしている個々のプラグイン リソースのバックアップ

どのリソース グループにも含まれていない、NetAppがサポートしているプラグイン リソースは、[Resources]ページから個別にバックアップすることができます。リソースのバックアップはオンデマンドで実行できるほか、リソースにポリシーが適用されてスケジュールが設定されていれば、スケジュールに従って自動的にバックアップが行われます。

開始する前に

- バックアップ ポリシーを作成しておく必要があります。
- セカンダリ ストレージとのSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

クリック  をクリックし、ホスト名とリソース タイプを選択してリソースをフィルターします。そのあとに  をクリックすると、フィルタ ペインが閉じます。

3. バックアップするリソースをクリックします。
4. [リソース] ページで、カスタム名を使用する場合は、[スナップショット コピーにカスタム名形式を使用する] チェック ボックスをオンにし、スナップショット名のカスタム名形式を入力します。

たとえば、`customtext_policy_hostname` または `resource_hostname` です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

5. [Application Settings] ページで、次の操作を実行します。
 - a. 追加のバックアップ オプションを設定するには、[バックアップ] 矢印をクリックします。必要に応じて、整合グループのバックアップを有効にし、次の操作を実行します。

フィールド	操作
Afford time to wait for Consistency Group Snapshot operation to complete	Snapshot処理が完了するまでの待機時間として、[Urgent]、[Medium]、または[Relaxed]のいずれかを選択します。 [Urgent]は5秒、[Medium]は7秒、[Relaxed]は20秒です。
Disable WAFL Sync	WAFL整合ポイントを強制しない場合はオンにします。

+

- a. *スクリプト*矢印をクリックして、静止、スナップショット、および静止解除操作の事前および事後コマンドを実行します。バックアップ処理を終了する前のプリコマンドも実行できます。

プリスクリプトとポストスクリプトはSnapCenter Serverで実行されます。

- b. *カスタム構成*矢印をクリックし、このリソースを使用するすべてのジョブに必要なカスタム値のペアを入力します。
- c. スナップショット コピー ツール の矢印をクリックして、スナップショットを作成するツールを選択します。

あなたが望むなら...	操作
SnapCenterでストレージ レベルのSnapshotを作成する	ファイル システムの整合性のないSnapCenter * を選択します。
SnapCenterでPlug-in for Windowsを使用してファイルシステムを整合性のある状態にしてからSnapshotを作成する	ファイル システムの一貫性を備えたSnapCenter * を選択します。
Snapshotを作成するためのコマンドを入力する	*その他*を選択し、スナップショットを作成するコマンドを入力します。

6. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックし  でポリシーを作成することもできます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、 をクリックします。
- c. ポリシー *policy_name* のスケジュールの追加ダイアログ ボックスでスケジュールを構成し、[OK] をクリックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

7. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP は、設定 > グローバル設定 でも設定する必要があります。

8. 概要を確認し、[完了] をクリックします。

リソースのトポロジ ページが表示されます。

9. *今すぐバックアップ*をクリックします。

10. [Backup]ページで次の手順を実行します。

- a. リソースに複数のポリシーを適用している場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ*をクリックします。

11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-smconnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\
```

ユーザ名とパスワードのプロンプトが表示されます。

2. Add-SmResourcesコマンドレットを使用して、リソースを追加します。

リソースを追加する例を次に示します。

```
Add-SmResource -HostName 'scc55.sscore.test.com' -PluginCode  
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database  
-StorageFootPrint (  
@{"VolumeName"="qtree_vol1_scc55_sscore_test_com";"QTREENAME"="qtree  
Vol1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. Add-SmPolicyコマンドレットを使用して、バックアップ ポリシーを作成します。

新しいバックアップ ポリシーを作成する例を示します。

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'  
-PluginPolicyType DummyPlugin -description 'testPolicy'
```

4. Add-SmResourceGroupコマンドレットを使用して、SnapCenterに新しいリソース グループを追加します。

この例では、ポリシーとリソースを指定して新しいリソース グループを作成しています。

```
Add-SmResourceGroup -ResourceGroupName  
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'  
-Resources  
@(@{"Host"="scc55.sscore.test.com";"Uid"="QTREE2";"PluginName"="Dumm  
yPlugin"},@{"Host"="scc55.sscore.test.com";"Uid"="QTREE";"PluginName  
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'  
-usesnapcenterwithoutfilesystemconsistency
```

5. New-SmBackupコマンドレットを使用して、新しいバックアップ ジョブを開始します。

```
New-SMBackup -DatasetName  
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy  
test2
```

6. Get-SmBackupReportコマンドレットを使用して、バックアップ ジョブのステータスを表示します。

この例では、指定した日に実行されたすべてのジョブの概要レポートを表示しています。

```
Get-SmBackupReport -JobId 149
```

```
BackedUpObjects      : {QTREE2, QTREE}
FailedObjects        : {}
IsScheduled           : False
HasMetadata           : False
SmBackupId            : 1
SmJobId               : 149
StartDateTime         : 1/15/2024 1:35:17 AM
EndDateTime          : 1/15/2024 1:36:19 AM
Duration              : 00:01:02.4265750
CreatedDateTime       : 1/15/2024 1:35:51 AM
Status                : Completed
ProtectionGroupName   :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows
SmProtectionGroupId   : 1
PolicyName            : test2
SmPolicyId            : 4
BackupName            :
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-
15-2024_01.35.17.4467
VerificationStatus    : NotApplicable
VerificationStatuses  :
SmJobError            :
BackupType            : SCC_BACKUP
CatalogingStatus      : NotApplicable
CatalogingStatuses   :
ReportDataCreatedDateTime :
PluginCode            : SCC
PluginName            : DummyPlugin
PluginDisplayName     : DummyPlugin
JobTypeId             :
JobHost               : scc55.sccore.test.com
```

NetAppがサポートしているプラグイン リソースのリソース グループのバックアップ

リソース グループは、[Resources]ページからオンデマンドでバックアップできます。リソース グループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従って自動的にバックアップが行われます。

開始する前に

- ポリシーを適用したリソース グループを作成しておく必要があります。
- セカンダリ ストレージにSnapMirror関係を持つリソースをバックアップする場合は、ストレージ ユーザ

ーに割り当てられたONTAPロールに「snapmirror all」権限が含まれている必要があります。ただし、「vsadmin」ロールを使用している場合は、「snapmirror all」権限は必要ありません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。

リソース グループを検索することができます。そのためには、検索ボックスにリソース グループ名を入力するか、 をクリックし、タグを選択します。そのあとに  をクリックすると、フィルタ ペインが閉じます。

3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] をクリックします。
4. [Backup] ページで次の手順を実行します。
 - a. リソース グループに複数のポリシーを関連付けている場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ* をクリックします。

5. モニター > ジョブ をクリックして、操作の進行状況を監視します。

- MetroCluster 構成では、フェイルオーバー後に SnapCenter で保護関係を検出できないことがあります。

"MetroClusterのフェイルオーバー後にSnapMirror関係またはSnapVault関係を検出できない"

- VMDK上のアプリケーション データをバックアップする場合に、SnapCenter Plug-in for VMware vSphereのJavaヒープ サイズが不足していると、バックアップが失敗することがあります。Javaヒープ サイズを増やすには、スクリプト ファイル/opt/netapp/init_scripts/scvserviceを探します。その脚本では、do_start method` コマンドは、 SnapCenter VMware プラグイン サービスを開始します。このコマンドを次のように更新します。`Java -jar -Xmx8192M -Xms4096M。

NetAppがサポートしているプラグインでのリソースのバックアップ処理の監視

SnapCenterの[Jobs]ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

-  進行中
-  正常に完了しました
-  失敗した

-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*ジョブ*をクリックします。
3. [Jobs]ページで、次の手順を実行します。
 - a. をクリックして、 リストの内容をバックアップ処理だけに絞り込みます。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*バックアップ*を選択します。
 - d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. バックアップ ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスは  ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

NetAppがサポートしているプラグインのバックアップ処理のキャンセル

キューに登録されているバックアップ処理はキャンセルできます。

必要なもの

- 処理をキャンセルするには、SnapCenter管理者かジョブ所有者としてログインする必要があります。
- バックアップ操作は、[モニター] ページまたは [アクティビティ] ペインからキャンセルできます。
- 実行中のバックアップ処理はキャンセルできません。
- バックアップ処理のキャンセルには、SnapCenter GUI、PowerShellコマンドレット、またはCLIコマンドを使用できます。
- キャンセルできない操作の場合、「ジョブのキャンセル」ボタンは無効になります。
- ロールの作成時に [ユーザー\グループ] ページで このロールのすべてのメンバーが他のメンバーのオブジェクトを表示および操作できる を選択した場合、そのロールの使用中に他のメンバーのキューに入れられたバックアップ操作をキャンセルできます。

手順

1. 次のいずれかを実行します。

方法	アクション
[Monitor]ページ	- 左側のナビゲーション ペインで、モニター > ジョブ をクリックします。 - 操作を選択し、「ジョブのキャンセル」をクリックします。
[Activity]ペイン	- バックアップ操作を開始したら、*をクリックします。 * アクティビティ ペインで、最新の 5 つの操作を表示します。 - 処理を選択します。 - ジョブの詳細ページで、「ジョブのキャンセル」をクリックします。

処理がキャンセルされ、リソースは処理前の状態に戻ります。

[Topology]ページでのNetAppがサポートしているプラグイン リソースに関連するバックアップとクローンの表示

リソースのバックアップまたはクローニングを準備する際に、プライマリ ストレージとセカンダリ ストレージ上のすべてのバックアップとクローンの図を表示すると役に立ちます。[Topology]ページでは、選択したリソースまたはリソース グループに使用できるバックアップとクローンをすべて表示できます。これらのバックアップとクローンの詳細を参照し、対象を選択してデータ保護処理を実行できます。

タスク概要

プライマリ ストレージまたはセカンダリ ストレージ（ミラー コピーまたはバックアップ コピー）にバックアップとクローンがあるかどうかは、[Manage Copies]ビューの次のアイコンで確認できます。

- 
 プライマリ ストレージで使用可能なバックアップとクローンの数を表示します。
- 
 SnapMirrorテクノロジーを使用してセカンダリ ストレージにミラーリングされているバックアップとクローンの数を表示します。
- 
 mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンもトポロジ ビューに表示されますが、トポロジ ビューのミラー バックアップの数には、バージョンに依存しないバックアップが含まれません。
- 
 SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップとクローンの数を表示します。

表示されるバックアップの数には、セカンダリ ストレージから削除されたバックアップも含まれます。た

例えば、4個のバックアップのみを保持するポリシーを使用して6個のバックアップを作成した場合、バックアップの数は6個と表示されます。



mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンもトポロジ ビューに表示されますが、トポロジ ビューのミラー バックアップの数には、バージョンに依存しないバックアップが含まれません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストからリソースまたはリソース グループを選択します。
3. リソースの詳細ビューまたはリソース グループの詳細ビューで、リソースを選択します。

リソースが保護されている場合は、選択したリソースのトポロジ ページが表示されます。

4. [Summary Card]で、プライマリ ストレージとセカンダリ ストレージ上にあるバックアップとクローンの数の概要を確認します。

[Summary Card]セクションには、バックアップとクローンの総数が表示されます。

更新ボタンをクリックすると、ストレージのクエリが実行されて正確な数が表示されます。

SnapLock対応バックアップが取得された場合、[更新] ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでも、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

アプリケーション リソースが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限はONTAPから取得されます。

オンデマンド バックアップ後、[更新] ボタンをクリックすると、バックアップまたはクローンの詳細が更新されます。

5. 「コピーの管理」ビューで、プライマリ ストレージまたはセカンダリ ストレージから バックアップ または クローンをクリックして、バックアップまたはクローンの詳細を表示します。

バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、名前変更、削除の各処理を実行します。



セカンダリ ストレージ システム上のバックアップは、名前変更または削除できません。



プライマリ ストレージ システムにあるバックアップは名前を変更できません。

7. クローンを削除する場合は、表でクローンを選択し、 をクリックして削除します。

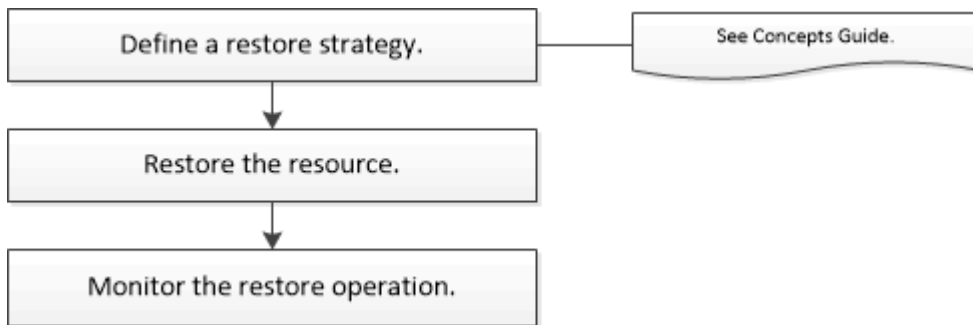
NetAppがサポートしているプラグイン リソースのリストア

NetAppがサポートしているプラグイン リソースのリストア

リストアとリカバリのワークフローには、計画、リストア処理の実行、および処理の監視が含まれます。

タスク概要

次のワークフローは、リストア処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトで使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、[SnapCenterコマンドレットのヘルプ](#)を使用するか、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

リソースのバックアップのリストア

SnapCenterを使用してリソースをリストアすることができます。リストア処理の機能は、使用するプラグインによって異なります。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- ユーザがSnapshotをミラーまたはバックアップにレプリケートする場合は、ソース ボリュームとデスティネーション ボリューム両方のStorage Virtual Machine (SVM) をSnapCenter管理者がユーザに割り当てる必要があります。
- リストアするリソースまたはリソース グループに対して現在実行中のバックアップ処理がある場合は、すべてキャンセルしておく必要があります。

タスク概要

- デフォルトのリストア処理でリストアされるのは、ストレージ オブジェクトのみです。アプリケーションレベルのリストア処理は、その機能がNetAppがサポートしているプラグインで提供されている場合にのみ実行できます。
- ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホストまたはクラスタ名、関連するリソース グループとポリシー、ステータスなどの情報とともに表示されます。



リストアの実行時は、バックアップがリストア グループに対するものであっても、リストア対象のリソースを個別に選択する必要があります。

リソースが保護されていない場合は、[全体的なステータス] 列に [保護されていません] と表示されます。

全体的なステータス 列のステータス「保護されていません」は、リソースが保護されていないか、リソースが別のユーザーによってバックアップされたことを意味します。

3. リソースを選択するか、リソース グループを選択してそのグループ内のリソースを選択します。

リソースのトポロジ ページが表示されます。

4. コピーの管理 ビューで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージ システムから バックアップ を選択します。
5. プライマリバックアップテーブルで、復元するバックアップを選択し、。



6. [復元範囲] ページで、[完全なリソース] または [ファイル レベル] のいずれかを選択します。
 - a. *完全なリソース*を選択した場合は、リソースのバックアップが復元されます。

リソースにストレージ容量としてボリュームまたはqtreeが含まれている場合、それらのボリュームまたはqtreeの以降のSnapshotは削除され、リカバリすることはできません。また、同じボリュームまたはqtreeで他のリソースがホストされている場合、そのリソースも削除されます。

- b. ファイル レベル を選択した場合は、すべて を選択するか、ボリュームまたは qtree を選択して、選択したボリュームまたは qtree に関連するパスをコンマで区切って入力できます。

- ボリュームとqtreeは複数選択できます。
- リソース タイプがLUNの場合は、LUN全体がリストアされます。複数のLUNを選択できます。+ 注意: すべて を選択すると、ボリューム、qtree、または LUN 上のすべてのファイルが復元されます。

7. 事前操作 ページで、復元ジョブを実行する前に実行する復元前コマンドとマウント解除コマンドを入力します。
8. **Post ops** ページで、復元ジョブを実行した後に実行するマウント コマンドと復元後のコマンドを入力します。
9. *通知*ページの*電子メール設定*ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP は、[設定] > [グローバル設定] ページでも設定する必要があります。

10. 概要を確認し、[完了] をクリックします。
11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

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

2. Get-SmBackupコマンドレットおよびGet-SmBackupReportコマンドレットを使用して、リストアする1つまたは複数のバックアップに関する情報を取得します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

この例では、2015年1月29日から2015年2月3日までのバックアップに関する詳細な情報を示しています。

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName        : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName        : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. Restore-SmBackupコマンドレットを使用して、バックアップからデータをリストアします。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

NetAppがサポートしているプラグインでのリソースのリストア処理の監視

[Job]ページを使用して、SnapCenterの各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター* ページで、*ジョブ* をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  でリストをフィルタリングし、リストア処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ* ドロップダウンリストから*復元*を選択します。
 - d. *ステータス* ドロップダウンリストから、復元ステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. 復元ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細* ページで、*ログの表示* をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

NetAppがサポートしているプラグイン リソースのバックアップのクローニング

NetAppがサポートしているプラグイン リソースのバックアップのクローニング

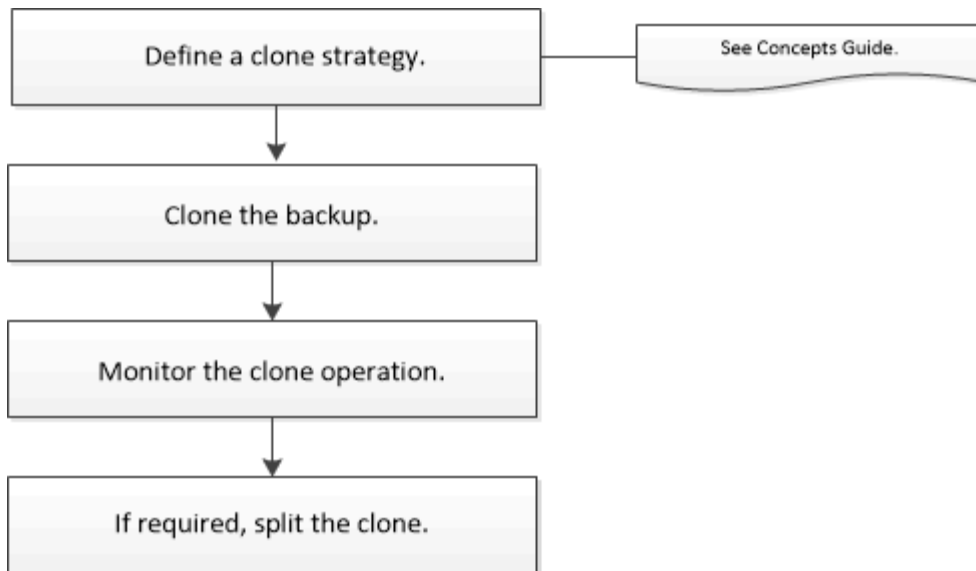
クローニング ワークフローには、クローニング処理の実行と処理の監視が含まれます。

タスク概要

リソースのバックアップをクローニングする理由には次のものがあります。

- アプリケーション開発のライフサイクルで、実装が必要な機能を、現在のリソースの構造およびコンテンツを使用してテストするため
- データの抽出と操作を行うツールで、データ ウェアハウスにデータを取り込むため
- 誤って削除または変更されたデータをリカバリするため

次のワークフローは、クローニング処理の実行順序を示しています。



PowerShellコマンドレットを手動またはスクリプトでを使用して、バックアップ、リストア、クローニングの処理を実行することもできます。PowerShellコマンドレットの詳細については、[SnapCenterコマンドレットのヘルプ](#)を使用するか、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)。

バックアップからのクローニング

SnapCenterを使用してバックアップをクローニングすることができます。クローニングはプライマリとセカンダリのどちらのバックアップからも実行できます。クローニング処理の機能は、使用するプラグインによって異なります。

開始する前に

- リソースまたはリソース グループをバックアップしておく必要があります。
- デフォルトのクローニング処理でクローニングされるのは、ストレージ オブジェクトのみです。アプリケーション レベルのクローニング処理は、その機能がNetAppがサポートしているプラグインで提供されている場合にのみ実行できます。
- ボリュームをホストするアグリゲートがStorage Virtual Machine (SVM) の割り当て済みアグリゲート リストに含まれていることを確認します。

タスク概要

ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

SnapCenter UI

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. リソース ページで、リソース タイプに基づいて 表示 ドロップダウン リストからリソースをフィルターします。

リソースは、タイプ、ホストまたはクラスタ名、関連するリソース グループとポリシー、ステータスなどの情報とともに表示されます。

3. リソースまたはリソース グループを選択します。

リソース グループを選択した場合はリソースを選択する必要があります。

リソースまたはリソース グループのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージ システムから [バックアップ] を選択します。
5. 表からデータバックアップを選択し、クリックします。 。
6. [Locations] ページで、次の操作を実行します。

フィールド	操作
Clone server	ソース ホストがデフォルトで入力されています。 別のホストを指定する場合は、クローンのマウント先の、プラグインがインストールされたホストを選択します。
Clone suffix	クローン デスティネーションがソースと同じ場合は必須です。 クローニングされた新しいリソース名に付けるサフィックスを入力します。サフィックスにより、クローニングされたリソースがホストで一意になります。 たとえば、rs1_cloneのように指定します。元のリソースと同じホストにクローニングする場合、クローニングされたリソースを元のリソースと区別するためにサフィックスを指定する必要があります。これを行わないと処理は失敗します。

リソースとしてLUNを選択し、セカンダリ バックアップからクローニングする場合、デスティネーション ボリュームのリストが表示されます。1つのソースについて複数のデスティネーション ボリュームを選択することができます。

7. *設定*ページで、次の操作を実行します。

フィールド	操作
イニシエーター名	ホスト イニシエーター名 (IQDNまたはWWPN)を入力します。
Igroup protocol	[Igroup protocol]を選択します。



[Settings]ページは、ストレージ タイプがLUNの場合にのみ表示されます。

8. [Scripts]ページで、クローニング処理の前後に実行するプリコマンドやポストコマンドを入力します。ホストにファイルシステムをマウントするには、mountコマンドを入力します。

例えば：

- クローニング前のコマンド：同じ名前の既存のデータベースの削除
- クローニング後のコマンド：データベースの検証やデータベースの起動

Linux マシン上のボリュームまたは qtree のマウント コマンド：
mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>

9. *通知*ページの*電子メール設定*ドロップダウンリストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。

10. 概要を確認し、[完了] をクリックします。

11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

PowerShellコマンドレット

手順

1. Open-SmConnectionコマンドレットを使用して、指定のユーザでSnapCenter Serverとの接続セッションを開始します。

```
Open-SmConnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146/
```

2. Get-SmBackupコマンドレットまたはGet-SmResourceGroupコマンドレットを使用して、クローニングできるバックアップのリストを表示します。

この例では、使用可能なすべてのバックアップに関する情報を表示しています。

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

この例では、指定したリソース グループに関する情報を表示しています。

```
PS C:\> Get-SmResourceGroup
```

```
Description :
CreationTime : 10/10/2016 4:45:53 PM
ModificationTime : 10/10/2016 4:45:53 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {}
HostResourceMapping : {}
Configuration :
SMCoreContracts.SmCloneConfiguration
LastBackupStatus : Completed
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo :
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Tag :
```

```

IsInternal                : False
EnableEmailAttachment     : False
VerificationSettings      : {}
Name                      : NFS_DB
Type                      : Group
Id                        : 2
Host                      :
UserName                  :
Passphrase                :
Deleted                   : False
Auth                      : SMCoreContracts.SmAuth
IsClone                   : False
CloneLevel                : 0
Hosts                     :
StorageName               :
ResourceGroupNames        :
PolicyNames               :

Description                :
CreationTime               : 10/10/2016 4:51:36 PM
ModificationTime           : 10/10/2016 5:27:57 PM
EnableEmail               : False
EmailSMTPServer            :
EmailFrom                  :
EmailTo                    :
EmailSubject               :
EnableSysLog               : False
ProtectionGroupType        : Backup
EnableAsupOnFailure        : False
Policies                   : {}
HostResourceMapping        : {}
Configuration              :
SMCoreContracts.SmCloneConfiguration
LastBackupStatus           : Failed
VerificationServer         :
EmailBody                  :
EmailNotificationPreference : Never
VerificationServerInfo     :
SchedulerSQLInstance       :
CustomText                  :
CustomSnapshotFormat       :
SearchResources            : False
ByPassRunAs                : False
IsCustomSnapshot           :
MaintenanceStatus          : Production
PluginProtectionGroupTypes : {SMSQL}

```

```

Tag                :
IsInternal          : False
EnableEmailAttachment : False
VerificationSettings : {}
Name                : Test
Type                : Group
Id                  : 3
Host                :
UserName            :
Passphrase          :
Deleted             : False
Auth                : SMCoreContracts.SmAuth
IsClone             : False
CloneLevel          : 0
Hosts                :
StorageName          :
ResourceGroupNames   :
PolicyNames          :

```

3. New-SmCloneコマンドレットを使用して、クローン リソース グループまたは既存のバックアップからクローニング処理を開始します。

この例では、指定したバックアップからすべてのログを含めてクローンを作成しています。

```

New-SmClone -BackupName
Verify_delete_clone_on_qtree_windows_scc54_10-04-2016_19.05.48.0886
-Resources @{"Host"="scc54.sccore.test.com";"Uid"="QTREE1"} -
CloneToInstance scc54.sccore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sccore.test.com' -igroupprotocol 'mixed'

```

4. クローニング ジョブのステータスを表示するには、Get-SmCloneReportコマンドレットを使用します。

この例では、指定したジョブIDのクローン レポートを表示しています。

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration             : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName           : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName     : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources      : {Don, Betty, Bobby, Sally}
ClonedResources      : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError           :
```

NetAppがサポートしているプラグインでのリソースのクローニング処理の監視

SnapCenterのクローニング処理の進捗状況を、[Jobs]ページで監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。

2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  てリストをフィルタリングし、クローニング処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*クローン*を選択します。
 - d. *ステータス*ドロップダウンリストからクローンのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. クローンジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. ジョブの詳細ページで、*ログの表示*をクリックします。

UNIXファイルシステムの保護

SnapCenter Plug-in for UNIX File Systemsの機能

Plug-in for UNIX File Systemsをインストールした環境では、SnapCenterを使用してUNIXファイルシステムをバックアップ、リストア、およびクローニングすることができます。これらの処理をサポートするタスクも実行できます。

- リソースの検出
- UNIXファイルシステムのバックアップ
- バックアップ処理のスケジュールの設定
- ファイルシステムのバックアップのリストア
- ファイルシステムのバックアップのクローニング
- バックアップ、リストア、クローニングの各処理を監視する

サポートされている構成

項目	サポートされる構成
環境	• 物理サーバ • 仮想サーバ NFSとSANの両方に存在するvVolデータストア。vVolデータストアは、ONTAP Tools for VMware vSphereでのみプロビジョニングできます。
オペレーティング システム	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
ファイルシステム	• SAN : ◦ LVMベースと非LVMベースの両方のファイルシステム ◦ VMDK ext3、ext4、xfs経由のLVM • NFS: NFS v3、NFS v4.x
プロトコル	• FC • FCoE • iSCSI • NFS

項目	サポートされる構成
マルチパス	はい

制限事項

- ボリューム グループでのRDMと仮想ディスクの混在はサポートされていません。
- ファイル レベルのリストアはサポートされていません。

ただし、バックアップをクローニングし、ファイルを手動でコピーすることで、ファイル レベルのリストアを手動で実行できます。

- NFSデータストアとVMFSデータストアの両方のVMDKにまたがるファイルシステムの混在はサポートされていません。
- NVMeはサポートされていません。
- プロビジョニングはサポートされていません。

機能

- LinuxまたはAIXシステム上の基盤となるホスト ストレージ スタックを処理することで、Plug-in for Oracle Databaseにより、Oracleデータベースに対してデータ保護処理を実行できるようになります。
- ONTAPを実行するストレージ システムで、Network File System（NFS）プロトコルとストレージ エリア ネットワーク（SAN）プロトコルがサポートされます。
- Linuxシステムでは、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録した場合、VMDKおよびRDM LUN上のOracleデータベースがサポートされます。
- SANファイルシステムおよびLVMレイアウトでAIXのマウント ガードがサポートされます。
- AIXシステムの場合のみ、Enhanced Journaled File System（JFS2）およびSANファイルシステムとLVM レイアウトでのインライン ロギングがサポートされます。

SANデバイス上に構築されたSANネイティブ デバイス、ファイルシステム、LVMレイアウトがサポートされます。

- SnapCenter環境のUNIXファイルシステムに対するアプリケーション対応のバックアップ、リストア、クローニングの各処理が自動化されます。

SnapCenter Plug-in for UNIX File Systemsのインストール

ホストを追加して**Plug-in Package for Linux**をインストールするための前提条件

ホストを追加してPlug-in Package for Linuxをインストールする前に、すべての要件を満たしておく必要があります。

- iSCSIを使用している場合は、iSCSIサービスが実行されている必要があります。
- パスワードベースの認証またはSSHキーベースの認証を使用できます。パスワードベースの認証はrootユーザとroot以外のユーザが使用できます。

SnapCenter Plug-in for UNIX File Systemsは、root以外のユーザもインストールできます。ただし、プラグイン プロセスをインストールして開始できるよう、root以外のユーザにsudo権限を設定する必要があります。プラグインのインストール後、プロセスは有効なroot以外のユーザとして実行されます。

- インストール ユーザのクレデンシャルを、認証モードをLinuxに設定して作成します。
- Java 11をLinuxホストにインストールしておく必要があります。



LinuxホストにJava 11の認定エディションのみがインストールされていることを確認します。

JAVA のダウンロードについては、以下を参照してください。 ["すべてのオペレーティング システム用のJavaのダウンロード"](#)

- プラグインのインストールには、デフォルトのシェルとして **bash** を使用する必要があります。

Linuxホストの要件

SnapCenter Plug-ins Package for Linuxをインストールする前に、ホストが要件を満たしていることを確認する必要があります。

項目	要件
オペレーティング システム	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
ホスト上のSnapCenterプラグインに必要な最小RAM	2 GB
ホスト上のSnapCenterプラグインに必要なインストールおよびログの最小スペース	2 GB 十分なディスク スペースを割り当てて、ログ フォルダによるストレージ消費を監視する必要があります。必要なログ スペースは、保護対象のエンティティの数とデータ保護処理の頻度によって異なります。十分なディスク スペースがない場合は、最近実行した処理のログが作成されません。

項目	要件
必要なソフトウェア パッケージ	Java 11 Oracle JavaおよびOpenJDK  LinuxホストにJava 11の認定エディションのみがインストールされていることを確認します。 Javaを最新バージョンにアップグレードした場合は、/var/opt/snapcenter/spl/etc/spl.propertiesにあるJAVA_HOMEオプションが正しいJavaバージョンと正しいパスに設定されていることを確認する必要があります。

サポートされているバージョンに関する最新情報については、 ["NetApp Interoperability Matrix Tool"](#)。

GUIを使用したホストの追加とPlug-ins Package for Linuxのインストール

[Add Host]ページを使用してホストを追加し、SnapCenter Plug-ins Package for Linuxをインストールできます。プラグインは、自動的にリモート ホストにインストールされます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. 上部の*管理対象ホスト*タブが選択されていることを確認します。
3. *[追加]*をクリックします。
4. [Hosts]ページで、次の操作を実行します。

フィールド	操作
ホストタイプ	ホストタイプとして*Linux*を選択します。
ホスト名	ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。 SnapCenterが機能するためには、DNSが適切に設定されている必要があります。そのため、FQDNを入力することを推奨します。 SnapCenterを使用してサブドメインの一部であるホストを追加する場合は、FQDNを指定する必要があります。

フィールド	操作
Credentials	作成したクレデンシャルの名前を選択するか、新しいクレデンシャルを作成します。 このクレデンシャルには、リモート ホストに対する管理者権限が必要です。詳細については、クレデンシャルの作成に関する情報を参照してください。 指定したクレデンシャルの名前にカーソルを合わせると、クレデンシャルの詳細を確認できます。  クレデンシャルの認証モードは、[Add Host]ウィザードで指定するホスト タイプによって決まります。

5. 「インストールするプラグインの選択」セクションで、「**Unix ファイル システム**」を選択します。

6. (オプション) [その他のオプション] をクリックします。

フィールド	操作
ポート	デフォルトのポート番号をそのまま使用するか、ポート番号を指定します。 デフォルトのポート番号は8145です。SnapCenter Serverがカスタム ポートにインストールされている場合は、そのポート番号がデフォルト ポートとして表示されます。  プラグインを手動でインストールしてカスタム ポートを指定した場合は、同じポートを指定する必要があります。そうしないと、処理が失敗します。
Installation Path	デフォルトのパスは <code>/opt/NetApp/snapcenter</code> です。 必要に応じて変更できます。カスタム パスを使用する場合は、sudoersのデフォルトのコンテンツがカスタム パスで更新されていることを確認してください。
Skip optional preinstall checks	プラグインを手動でインストール済みで、プラグインをインストールするための要件をホストが満たしているかどうかを検証しない場合は、このチェックボックスをオンにします。

7. *送信*をクリックします。

[Skip prechecks]チェック ボックスをオンにしていない場合、プラグインをインストールするための要件を満たしているかどうかを確認するために、ホストが検証されます。



事前確認スクリプトでは、ファイアウォールの拒否ルールに指定されているプラグイン ポートのファイアウォール ステータスは検証されません。

最小要件を満たしていない場合、エラーまたは警告メッセージが表示されます。エラーがディスク容量または RAM に関連している場合は、`C:\Program Files\NetApp\ SnapCenter WebApp` にある `web.config` ファイルを更新してデフォルト値を変更できます。エラーが他のパラメータに関連している場合は、問題を修正する必要があります。



HAのセットアップでweb.configファイルを更新する場合は、両方のノードでファイルを更新する必要があります。

8. 指紋を確認して、「確認して送信」をクリックします。



SnapCenterでは、ECDSAアルゴリズムがサポートされていません。



前述の手順で同じホストがSnapCenterに追加され、フィンガープリントが確認された場合でも、フィンガープリントの検証は必須です。

9. インストールの進捗状況を監視します。

インストール固有のログ ファイルは、`/custom_location/snapcenter/logs` にあります。

結果

ホストにマウントされているすべてのファイルシステムが自動的に検出され、[Resources]ページに表示されます。何も表示されない場合は、[リソースの更新] をクリックします。

インストール ステータスの監視

[Jobs]ページを使用して、SnapCenterプラグイン パッケージのインストールの進捗状況を監視できます。インストールの進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

- 進行中
- 正常に完了しました
- 失敗した
- 警告付きで完了したか、警告のため開始できませんでした
- キューに登録

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、プラグインのインストール操作のみがリストされるようにリストをフィルタリングするには、次の手順を実行します。
 - a. *フィルター*をクリックします。
 - b. オプション：開始日と終了日を指定します。
 - c. [タイプ] ドロップダウン メニューから、[プラグインのインストール] を選択します。
 - d. [Status]ドロップダウン メニューから、インストールのステータスを選択します。
 - e. *適用*をクリックします。
4. インストール ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

SnapCenter Plug-in Loaderサービスの設定

SnapCenterプラグインLoaderサービスは、Linux がSnapCenterサーバーと対話するためのプラグイン パッケージをロードします。SnapCenter Plug-in Loaderサービスは、SnapCenter Plug-ins Package for Linuxのインストール時にインストールされます。

このタスクについて

SnapCenter Plug-ins Package for Linuxのインストール後に、SnapCenter Plug-in Loaderサービスが自動的に開始されます。SnapCenter Plug-in Loaderサービスが自動的に開始されない場合は、次の作業を行う必要があります。

- プラグインが動作しているディレクトリが削除されていないことを確認します。
- Java仮想マシンに割り当てられているメモリ容量を増やします。

`/custom_location/ NetApp/snapcenter/spl/etc/`にある `spl.properties` ファイルには、次のパラメータが含まれています。これらのパラメータにはデフォルト値が割り当てられています。

パラメータ名	説明
LOG_LEVEL	サポートされるログ レベルを表示します。 有効な値は、TRACE、DEBUG、INFO、WARN、ERROR、およびFATALです。
SPL_PROTOCOL	SnapCenter Plug-in Loaderでサポートされるプロトコルを表示します。 HTTPSプロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。

パラメータ名	説明
SNAPCENTER_SERVER_PROTOCOL	SnapCenter Serverでサポートされるプロトコルを表示します。 HTTPSプロトコルのみがサポートされています。デフォルト値がない場合は、値を追加できます。
SKIP_JAVAHOME_UPDATE	SPLサービスはデフォルトでjavaパスを検出し、JAVA_HOMEパラメータを更新します。 したがって、デフォルト値はFALSEに設定されます。デフォルトの動作を無効にしてjavaパスを手動で修正するには、TRUEに設定します。
SPL_KEYSTORE_PASS	キーストア ファイルのパスワードを表示します。 この値は、パスワードを変更する場合や新しいキーストア ファイルを作成する場合にのみ変更できます。
SPL_PORT	SnapCenter Plug-in Loaderサービスが実行されているポート番号を表示します。 デフォルト値がない場合は、値を追加できます。  プラグインのインストール後に値を変更しないでください。
SNAPCENTER_SERVER_HOST	SnapCenter ServerのIPアドレスまたはホスト名を表示します。
SPL_KEYSTORE_PATH	キーストア ファイルの絶対パスを表示します。
SNAPCENTER_SERVER_PORT	SnapCenter Serverが実行されているポート番号を表示します。

パラメータ名	説明
LOGS_MAX_COUNT	/custom_location/snapcenter/spl/logs フォルダに保存されているSnapCenterプラグLoaderログ ファイルの数を表示します。 デフォルト値は5000に設定されています。この数が指定した値より大きい場合は、最後に変更されたものから5,000個のファイルが保持されます。ファイル数のチェックは、SnapCenter Plug-in Loaderサービスが開始された時点から24時間ごとに自動的行われます。  spl.properties ファイルを手動で削除する場合、保持されるファイル数は9999に設定されます。
JAVA_HOME	SPLサービスの開始に使用されるJAVA_HOMEディレクトリの絶対パスを表示します。 このパスは、インストール時にSPLを開始する段階で決定されます。
LOG_MAX_SIZE	ジョブ ログ ファイルの最大サイズを表示します。 最大サイズに達すると、そのログ ファイルはzipされ、そのジョブの新しいファイルにログが書き込まれます。
RETAIN_LOGS_OF_LAST_DAYS	ログが保持される最大日数が表示されます。
ENABLE_CERTIFICATE_VALIDATION	ホストでCA証明書の検証が有効になっている場合はtrueと表示されます。 このパラメータを有効または無効にするには、spl.propertiesを編集するか、SnapCenterのGUIまたはコマンドレットを使用します。

これらのパラメータにデフォルト値が割り当てられていない場合や、値を割り当てたり変更したりする場合は、spl.propertiesファイルを変更できます。パラメータに割り当てられている値に関連する問題をトラブルシューティングするために、spl.propertiesファイルを検証および編集することもできます。spl.propertiesファイルを変更したら、SnapCenter Plug-in Loaderサービスを再起動する必要があります。

手順

- 必要に応じて、次のいずれかの操作を実行します。
 - SnapCenterプラグインLoaderサービスを開始します。
 - ルートユーザーとして、次を実行します:

```
/custom_location/NetApp/snapcenter/spl/bin/spl start
```

- 非ルートユーザーとして、次を実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
- SnapCenterプラグインLoaderサービスを停止します。
 - ルートユーザーとして、次を実行します: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
 - 非ルートユーザーとして、次を実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`



stopコマンドで-forceオプションを使用すると、SnapCenter Plug-in Loaderサービスを強制的に停止できます。ただし、既存の処理も終了してしまうため、このコマンドを使用する際は十分に注意してください。

- SnapCenterプラグインLoaderサービスを再起動します。
 - ルートユーザーとして、次を実行します: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
 - 非ルートユーザーとして、次を実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
- SnapCenterプラグインLoaderサービスのステータスを確認します。
 - ルートユーザーとして、次を実行します: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
 - 非ルートユーザーとして、次を実行します: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
- SnapCenterプラグインLoaderサービスの変更を見つけます。
 - ルートユーザーとして、次を実行します: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
 - 非ルートユーザーとして、次を実行します。 `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

LinuxホストでのSnapCenter Plug-in Loader (SPL) サービスを使用したCA証明書の設定

インストールされたデジタル証明書をアクティブ化するには、SnapCenterプラグインLoaderサービスを使用して、SPL キーストアとその証明書のパスワードを管理し、CA 証明書を構成し、SPL 信頼ストアにルート証明書または中間証明書を構成し、CA 署名キー ペアを SPL 信頼ストアに構成する必要があります。



SPLでは、「/var/opt/snapcenter/spl/etc」にある「keystore.jks」ファイルを、トラストストアとキーストアのどちらにも使用します。

SPLキーストアのパスワードと、使用中のCA署名キー ペアのエイリアスの管理

手順

1. SPLキーストアのデフォルト パスワードは、SPLプロパティ ファイルから取得できます。

これは、キー「SPL_KEYSTORE_PASS」に対応する値です。

2. キーストアのパスワードを変更します。

```
keytool -storepasswd -keystore keystore.jks
```

・ キーストア内の秘密キー
エントリのすべてのエイリアスのパスワードを、キーストアと同じパスワードに変更します。

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

spl.propertiesファイルのキーSPL_KEYSTORE_PASSについても、同様に更新します。

3. パスワードを変更したら、サービスを再起動します。



SPLキーストアのパスワードと、秘密キーに関連付けられているエイリアス パスワードをすべて同じにする必要があります。

ルート証明書または中間証明書のSPLトラストストアへの設定

ルート証明書や中間証明書は、SPLトラストストアへの秘密キーなしで設定する必要があります。

手順

1. SPL キーストアが格納されているフォルダー (/var/opt/snapcenter/spl/etc) に移動します。
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

・ ルート証明書か中間証明書を追加します。

```
keytool -import -trustcacerts -alias  
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore  
keystore.jks
```

・
SPLトラストストアへのルート証明書または中間証明書を設定したら、サービスを再起動します。
。



ルートCA証明書を追加してから、中間CA証明書を追加する必要があります。

SPLトラストストアに対するCA署名付きキー ペアの設定

SPLトラストストアに対してCA署名付きキー ペアを設定する必要があります。

手順

1. SPLキーストアが格納されているフォルダに移動します：/var/opt/snapcenter/spl/etc
2. 「keystore.jks」 ファイルを探します。
3. キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

- ・ 秘密キーと公開キーの両方が設定されたCA証明書を追加します。

```
keytool -importkeystore -srckeystore <CertificatePathToImport>  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

- ・ キーストアに追加された証明書の一覧を表示します。

```
keytool -list -v -keystore keystore.jks
```

- ・ キーストアに追加された新しい
CA証明書に対応するエイリアスが、キーストアに含まれていることを確認します。
- ・ CA証明書に追加した秘密キーのパスワードを、キーストアのパスワードに変更します。

SPLキーストアのデフォルトのパスワードは、spl.propertiesファイルのキーSPL_KEYSTORE_PASSの値です。

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore  
keystore.jks
```

- ・ CA 証明書のエイリアス名が長く、スペースや特殊文字（「*」、「」）
が含まれている場合は、エイリアス名を単純な名前に変更します。

```
keytool -changealias -alias "<OriginalAliasName>" -destalias  
"<NewAliasName>" -keystore keystore.jks
```

- ・ spl.propertiesファイルにあるキーストアからエイリアス名を設定します。

SPL_CERTIFICATE_ALIASキーに対するこの値を更新します。

4. SPLトラストストアにCA署名キー ペアを設定したら、サービスを再起動します。

SPLの証明書失効リスト（CRL）の設定

SPLにCRLを設定する必要があります。

このタスクについて

- SPLは、あらかじめ設定されたディレクトリでCRLファイルを検索します。
- SPL の CRL ファイルのデフォルト ディレクトリは `/var/opt/snapcenter/spl/etc/crl` です。

手順

1. キーSPL_CRL_PATHに照らしてspl.propertiesファイルのデフォルト ディレクトリを変更および更新できます。
2. このディレクトリには、複数のCRLファイルを格納できます。

受信する証明書については、それぞれのCRLに対して検証が行われます。

プラグインのCA証明書の有効化

CA証明書を設定し、SnapCenter Serverと対応するプラグイン ホストに導入する必要があります。プラグインでCA証明書の検証を有効にする必要があります。

開始する前に

- 実行 `Set-SmCertificateSettings` コマンドレットを使用して、CA 証明書を有効または無効にすることができます。
- `Get-SmCertificateSettings` を使用して、プラグインの証明書の状態を表示できます。

コマンドレットで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. プラグイン ホストを1つまたは複数選択します。
4. *その他のオプション*をクリックします。
5. *証明書の検証を有効にする*を選択します。

終了後の操作

[Managed Hosts]タブのホストに鍵マークが表示されます。この鍵マークの色は、SnapCenter Serverとプラグイン ホスト間の接続のステータスを示します。

- *🔑* は、CA 証明書が有効になっていないか、プラグイン ホストに割り当てられていないことを示します。
- *🟢* は CA 証明書が正常に検証されたことを示します。
- *🔴* は、CA 証明書を検証できなかったことを示します。
- *🔒* は接続情報を取得できなかったことを示します。



ステータスが黄色または緑の場合は、データ保護処理が正常に完了しています。

SnapCenter Plug-in for VMware vSphereのインストール

データベースまたはファイルシステムが仮想マシン（VM）に格納されている場合や、VMとデータストアを保護する場合は、SnapCenter Plug-in for VMware vSphere仮想アプライアンスを導入する必要があります。

展開方法については、["導入プロセスの概要"](#)。

CA証明書を導入する

SnapCenter Plug-in for VMware vSphereで CA 証明書を構成するには、以下を参照してください。 ["SSL証明書を作成またはインポートする"](#)。

CRLファイルを設定する

SnapCenter Plug-in for VMware vSphereは、事前に設定されたディレクトリでCRLファイルを探します。SnapCenter Plug-in for VMware vSphere のCRL ファイルのデフォルト ディレクトリは `/opt/netapp/config/crl` です。

このディレクトリには、複数のCRLファイルを格納できます。受信する証明書については、それぞれのCRLに対して検証が行われます。

UNIXファイルシステムの保護の準備

バックアップ、クローニング、リストアなどのデータ保護処理を実行する前に、環境をセットアップする必要があります。SnapMirrorテクノロジーとSnapVaultテクノロジーを使用できるようにSnapCenter Serverをセットアップすることもできます。

SnapVaultテクノロジーとSnapMirrorテクノロジーを利用するには、ストレージ デバイス上のソース ボリュームとデスティネーション ボリュームの間にデータ保護関係を設定し、初期化する必要があります。この作業を実行するには、NetApp System Managerを使用するか、ストレージ コンソールのコマンドラインを使用します。

ユーザがPlug-in for UNIX File Systemsを使用するためには、SnapCenter管理者が事前にSnapCenter Serverをインストールして設定し、前提条件となるタスクを実行する必要があります。

- SnapCenter Server をインストールして構成します。 ["詳細情報"](#)
- ストレージ システム接続を追加して、 SnapCenter環境を構成します。 ["詳細情報"](#)



SnapCenterでは、別々のクラスタに属している場合でも、複数のSVMに同じ名前を付けることはサポートされません。SVMの登録またはクラスタの登録を使用してSnapCenterに登録されるSVMは、それぞれ一意である必要があります。

- ホストを追加し、プラグインをインストールし、リソースを検出します。
- SnapCenter Serverを使用してVMware RDM LUNまたはVMDK上のUNIXファイルシステムを保護する場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。
- LinuxホストにJavaをインストールします。

- バックアップ レプリケーションが必要な場合は、ONTAPでSnapMirrorとSnapVaultを設定します。

UNIXファイルシステムのバックアップ

バックアップに使用できるUNIXファイルシステムの検出

プラグインをインストールすると、そのホスト上のすべてのファイルシステムが自動検出されて[Resources]ページに表示されます。これらのファイルシステムをリソース グループに追加してデータ保護処理を実行できます。

開始する前に

- SnapCenter Serverのインストール、ホストの追加、ストレージ システム接続の作成などのタスクを完了しておく必要があります。
- ファイルシステムが仮想マシン ディスク (VMDK) またはrawデバイス マッピング (RDM) にある場合は、SnapCenter Plug-in for VMware vSphereを導入してSnapCenterに登録する必要があります。

詳細については、以下を参照してください。 ["SnapCenter Plug-in for VMware vSphereの導入"](#)。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから パス を選択します。
3. *リソースの更新*をクリックします。

ファイルシステムは、タイプ、ホスト名、関連するリソース グループとポリシー、ステータスなどの情報とともに表示されます。

UNIXファイルシステムのバックアップ ポリシーの作成

SnapCenterを使用してUNIXファイルシステムをバックアップする前に、バックアップ対象のリソースまたはリソース グループのバックアップ ポリシーを作成する必要があります。バックアップ ポリシーとは、バックアップをどのように管理し、スケジューリングし、保持するかを定める一連のルールです。レプリケーション、スクリプト、バックアップ タイプの設定を指定することもできます。ポリシーを作成することで、別のリソースやリソース グループでポリシーを再利用したい場合に時間を節約できます。

開始する前に

- SnapCenterのインストール、ホストの追加、ファイルシステムの検出、ストレージ システム接続の作成などのタスクを実行して、データ保護の準備をしておく必要があります。
- Snapshotをミラー セカンダリ ストレージまたはバックアップ セカンダリ ストレージにレプリケートするユーザには、SnapCenter管理者がソースとデスティネーションの両方のボリューム用にSVMを割り当てる必要があります。
- SnapMirrorアクティブ同期に固有の前提条件と制限事項を確認します。詳細については、 ["SnapMirrorアクティブ同期のオブジェクト数の制限"](#)。

タスク概要

- SnapLock

- [Retain the backup copies for a specific number of days]オプションを選択した場合は、SnapLockの保持期間をここで指定した保持日数以下にする必要があります。

Snapshotのロック期間を指定すると、保持期間が終了するまでSnapshotが削除されません。その結果、ポリシーで指定した数よりも多くのSnapshotが保持される可能性があります。

ONTAP 9.12.1以前のバージョンでは、リストアの一環としてSnapLock Vault Snapshotから作成されたクローンが、SnapLock Vaultの有効期限を継承します。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[ポリシー]をクリックします。
3. ドロップダウンリストから*Unix ファイル システム*を選択します。
4. *新規*をクリックします。
5. 「名前」 ページで、ポリシー名と詳細を入力します。
6. 「バックアップとレプリケーション」 ページで、次のアクションを実行します。
 - a. バックアップ設定を指定します。
 - b. オンデマンド、時間別、日次、週次、または*月次*を選択して、スケジュールの頻度を指定します。
 - c. [セカンダリ レプリケーション オプションの選択] セクションで、次のセカンダリ レプリケーション オプションの 1 つまたは両方を選択します。

フィールド	操作
Update SnapMirror after creating a local Snapshot copy	別のボリュームにバックアップ セットのミラー コピーを作成する場合（SnapMirrorレプリケーション）は、このフィールドを選択します。 このオプションは、SnapMirrorアクティブ同期に対して有効にする必要があります。
Update SnapVault after creating a local Snapshot copy	ディスクツーディスクのバックアップ レプリケーション（SnapVaultバックアップ）を実行する場合は、このオプションを選択します。
Error retry count	処理が停止されるまでに試行できるレプリケーションの最大回数を入力します。

7. [保持] ページで、[バックアップとレプリケーション] ページで選択したバックアップ タイプとスケジュール タイプの保持設定を指定します。

状況	操作

特定の数のSnapshotを保持	*保持するコピー*を選択し、保持するスナップショットの数を指定します。 Snapshotの数が指定した数を超えると、古いものから順にSnapshotが削除されます。  最大保持値は 1018 です。保持数を、使用しているONTAPバージョンがサポートする値よりも大きい値に設定すると、バックアップが失敗します。  SnapVaultレプリケーションを有効にする場合は、保持数を2以上に設定する必要があります。保持数を1に設定すると、新しいSnapshotがターゲットにレプリケートされるまで最初のSnapshotがSnapVault関係の参照Snapshotになるため、保持処理が失敗することがあります。
Snapshotを特定の日数だけ保持	*コピーの保持期間*を選択し、スナップショットを削除する前に保持する日数を指定します。
スナップショットコピーのロック期間	スナップショット コピーのロック期間 を選択し、期間を日数、月数、または年数で指定します。 SnapLock保持期間は100年未満にする必要があります。

8. ポリシーラベルを選択します。



リモート レプリケーションのプライマリ スナップショットにSnapMirrorラベルを割り当てることで、プライマリ スナップショットによってスナップショット レプリケーション操作をSnapCenterからONTAPセカンダリ システムにオフロードできるようになります。これは、ポリシー ページでSnapMirrorまたはSnapVaultオプションを有効にしなくても実行できます。

9. [Script]ページで、バックアップ処理の前またはあとに実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。



`_ /opt/ NetApp/snapcenter/scc/etc/allowed_commands.config_` パスからプラグイン ホスト上で使用可能なコマンド リストにコマンドが存在するかどうかを確認する必要があります。

スクリプトのタイムアウト値を指定することもできます。デフォルト値は60秒です。

10. 概要を確認し、[完了] をクリックします。

UNIXファイルシステムのリソース グループの作成とポリシーの適用

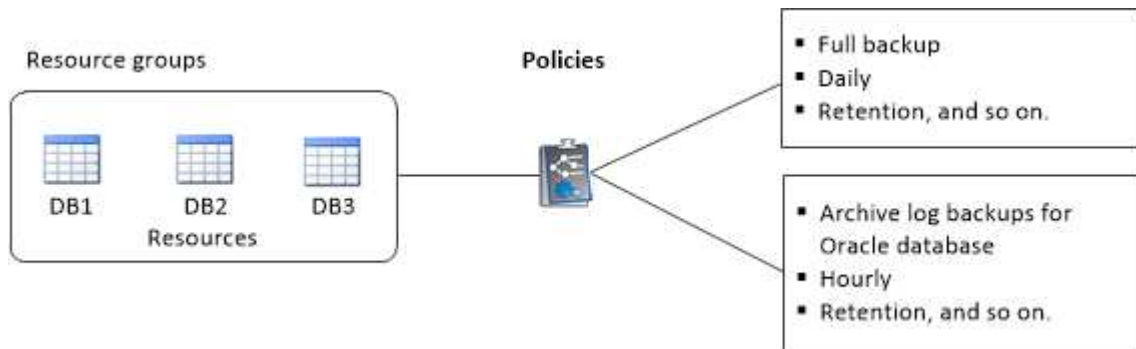
リソース グループはコンテナであり、バックアップして保護するリソースをここに追加します。リソース グループを使用することで、ファイルシステムに関連付けられているすべてのデータをバックアップできます。

タスク概要

- Oracle DBVERIFYユーティリティを使用してバックアップを検証するには、ASMディスク グループにファイルが格納されているデータベースが「MOUNT」または「OPEN」状態である必要があります。

リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義します。

次の図は、データベースのリソース、リソース グループ、ポリシーの関係を示しています。



- SnapLockが有効なポリシーの場合、ONTAP 9.12.1以前のバージョンでは、Snapshotのロック期間を指定すると、リストアの一環として改ざん防止Snapshotから作成されたクローンにSnapLockの有効期限が継承されます。SnapLockの有効期限が過ぎたあと、ストレージ管理者がクローンを手動でクリーンアップする必要があります。
- SnapMirrorアクティブ同期を使用しない新しいファイルシステムを、SnapMirrorアクティブ同期を使用するリソースを含む既存のリソース グループに追加することはできません。
- SnapMirrorアクティブ同期のフェイルオーバー モードである既存のリソース グループに新しいファイルシステムを追加することはできません。リソースを追加できるのは、通常の状態またはフェイルバック状態のリソース グループのみです。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。

- a. [Name] フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag] フィールドに1つ以上のラベルを入力します。

たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

- c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を

入力します。

たとえば、`customtext_resource group_policy_hostname`や`resource group_hostname`などの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

4. [リソース] ページで、[ホスト] ドロップダウン リストから Unix ファイル システムのホスト名を選択します。



[Available Resources]セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources]のリストには表示されません。

5. [Available Resources]セクションでリソースを選択し、[Selected Resources]セクションに移動します。

6. [Application Settings]ページで、次の操作を実行します。

- [Scripts]の矢印を選択し、休止、Snapshot、および休止解除の処理を行うプリコマンドとポストコマンドを入力します。障害の発生時に終了前に実行するプリコマンドも入力できます。
- 次のいずれかのバックアップ整合性オプションを選択します。
 - バックアップを作成する前にファイル システムのキャッシュ データがフラッシュされ、バックアップの作成中にファイル システムで入出力操作が許可されないようにするには、[ファイル システムの一貫性] を選択します。



[File System Consistent]を選択した場合、ボリューム グループに含まれるLUNに対して整合グループSnapshotが作成されます。

- バックアップを作成する前にファイル システムのキャッシュ データがフラッシュされるようにする場合は、クラッシュ整合性 を選択します。



リソース グループに複数の異なる種類のファイルシステムを追加した場合は、リソース グループ内の各種ファイルシステムのすべてのボリュームが整合グループに追加されます。

7. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックし  でポリシーを作成することもできます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、  をクリックします。
- c. ポリシー `policy_name` のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリックします。

ここで、`policy_name` は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

9. 概要を確認し、[完了] をクリックします。

ASA r2 システム上の Unix ファイルシステムのリソースグループを作成し、二次保護を有効にします。

ASA r2 システム上にあるリソースを追加するには、リソース グループを作成する必要があります。リソース グループの作成時にセカンダリ保護をプロビジョニングすることもできます。

開始する前に

- ONTAP 9.x リソースとASA r2 リソースの両方を同じリソース グループに追加していないことを確認する必要があります。
- ONTAP 9.x リソースとASA r2 リソースの両方を含むデータベースが存在しないことを確認する必要があります。

タスク概要

- 二次保護は、ログインしたユーザーに **SecondaryProtection** 機能が有効になっているロールが割り当てられている場合にのみ使用できます。
- セカンダリ保護を有効にすると、プライマリおよびセカンダリ整合性グループの作成中にリソース グループはメンテナンス モードになります。プライマリおよびセカンダリのコンシステンシー グループが作成されると、リソース グループのメンテナンス モードが解除されます。
- SnapCenter はクローン リソースの二次保護をサポートしていません。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。
 - a. [Name] フィールドにリソース グループの名前を入力します。



リソース グループ名は250文字以内で指定する必要があります。

- b. あとでリソース グループを検索できるように、[Tag] フィールドに1つ以上のラベルを入力します。

たとえば、複数のリソース グループにHRをタグとして追加すると、あとからHRタグに関連付けられたすべてのリソース グループを検索できます。

- c. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

たとえば、customtext_resource group_policy_hostnameやresource group_hostnameなどの形式です。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。

- d. バックアップの対象から外すアーカイブ ログ ファイルのデスティネーションを指定します。



必要に応じて、プレフィックスを含め、アプリケーションで設定されたのと同じ宛先を使用する必要があります。

- 4. [リソース] ページで、[ホスト] ドロップダウン リストからデータベース ホスト名を選択します。



[Available Resources]セクションには、正常に検出されたリソースのみがリストされます。最近追加したリソースは、ユーザがリソース リストを更新するまで[Available Resources]のリストには表示されません。

- 5. [使用可能なリソース] セクションからASA r2 リソースを選択し、[選択したリソース] セクションに移動します。
- 6. アプリケーション設定ページで、バックアップ オプションを選択します。
- 7. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。



をクリックし  でポリシーを作成することもできます。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. スケジュールを設定するポリシーの[Configure Schedules]列で、  をクリックします。
- c. ポリシー *policy_name* のスケジュールの追加ウィンドウでスケジュールを構成し、[OK] をクリックします。

ここで、*policy_name* は選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

サードパーティのバックアップ スケジュールは、SnapCenterのバックアップ スケジュールと重複している場合、サポートされません。

- 8. 選択したポリシーに対して二次保護が有効になっている場合は、「二次保護」 ページが表示されるので、次の手順を実行する必要があります。
- a. レプリケーション ポリシーのタイプを選択します。



同期レプリケーション ポリシーはサポートされていません。

- b. 使用する整合性グループのサフィックスを指定します。

- c. [宛先クラスタ] および [宛先 SVM] ドロップダウンから、使用するピア クラスタと SVM を選択します。



クラスタと SVM のピアリングはSnapCenterではサポートされていません。クラスタと SVM のピアリングを実行するには、System Manager またはONTAP CLI を使用する必要があります。



リソースがSnapCenterの外部ですでに保護されている場合、それらのリソースは [セカンダリ保護リソース] セクションに表示されます。

1. [Verification]ページで、次の手順を実行します。
 - a. ロケータのロード をクリックして、 SnapMirrorまたはSnapVaultボリュームをロードし、セカンダリストレージで検証を実行します。
 - b. クリック  ポリシーのすべてのスケジュール タイプの検証スケジュールを構成するには、[スケジュールの構成] 列で をクリックします。
 - c. [Add Verification Schedules policy_name]ダイアログ ボックスで、次の操作を実行します。

状況	操作
バックアップ後に検証を実行	*バックアップ後に検証を実行*を選択します。
検証のスケジュールを設定	*スケジュールされた検証を実行*を選択し、ドロップダウン リストからスケジュールの種類を選択します。

- d. セカンダリ ストレージ システム上のバックアップを検証するには、[セカンダリ ロケーションで検証] を選択します。
 - e. [OK]をクリックします。

設定した検証スケジュールが、[Applied Schedules]列にリストされます。

2. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースグループで実行された操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

3. 概要を確認し、[完了] をクリックします。

UNIXファイルシステムのバックアップ

どのリソース グループにもまだ含まれていないリソースは、[Resources]ページからバックアップすることができます。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから パス を選択します。
3. クリック  をクリックし、ホスト名と Unix ファイル システムを選択してリソースをフィルターします。
4. バックアップするファイルシステムを選択します。
5. [Resources] ページで実行できる手順は次のとおりです。
 - a. Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

例えば、`customtext_policy_hostname``または ``resource_hostname`。デフォルトでは、Snapshotの名前の後ろにタイムスタンプが付加されます。
6. [Application Settings] ページで、次の操作を実行します。
 - [Scripts]の矢印を選択し、休止、Snapshot、および休止解除の処理を行うプリコマンドとポストコマンドを入力します。障害の発生時に終了前に実行するプリコマンドも入力できます。
 - 次のいずれかのバックアップ整合性オプションを選択します。
 - バックアップを作成する前にファイル システムのキャッシュ データがフラッシュされ、バックアップの作成中にファイル システムで操作が実行されないようにするには、[ファイル システムの整合性] を選択します。
 - バックアップを作成する前にファイル システムのキャッシュ データがフラッシュされるようにする場合は、クラッシュ整合性 を選択します。
7. [Policies] ページで、次の手順を実行します。
 - a. ドロップダウン リストから1つ以上のポリシーを選択します。



クリックするとポリシーを作成できます 。

[Configure schedules for selected policies]セクションに、選択したポリシーがリストされます。

- b. クリック  必要なポリシーのスケジュールを構成するには、[スケジュールの構成] 列をクリックします。
- c. 「ポリシー_policy_name_のスケジュールを追加」ウィンドウでスケジュールを設定し、OK。

policy_name は、選択したポリシーの名前です。

設定したスケジュールが[Applied Schedules]列にリストされます。

8. 通知ページで、*電子メール設定*ドロップダウンリストから電子メールを送信するシナリオを選択します。

送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。リソースに対して実行されたバックアップ操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



電子メール通知の場合は、GUIまたはPowerShellコマンドを使用してSMTPサーバーの詳細を指定する必要があります。 `Set-SmSmtServer`。

9. 概要を確認し、[完了] をクリックします。

トポロジ ページが表示されます。

10. *今すぐバックアップ* をクリックします。

11. [Backup] ページで次の手順を実行します。

- a. リソースに複数のポリシーを適用した場合は、バックアップに使用するポリシーを[Policy] ドロップダウン リストから選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ* をクリックします。

12. モニター > ジョブ をクリックして、操作の進行状況を監視します。

UNIXファイルシステム リソース グループのバックアップ

リソース グループに定義されているUNIXファイルシステムをバックアップできます。リソース グループは、[Resources] ページからオンデマンドでバックアップできます。リソース グループにポリシーが適用され、かつスケジュールが設定されている場合は、スケジュールに従ってバックアップが作成されます。

手順

1. 左側のナビゲーション ペインで、リソース を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。
3. 検索ボックスにリソースグループ名を入力するか、 をクリックして、タグを選択します。

 をクリックし  でフィルタ ペインを閉じます。

4. [Resource Group] ページで、バックアップするリソース グループを選択します。
5. [Backup] ページで次の手順を実行します。
 - a. リソース グループに複数のポリシーが関連付けられている場合は、[ポリシー] ドロップダウン リストから使用するバックアップ ポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

- b. *バックアップ* を選択します。

6. モニター > ジョブ を選択して進行状況を監視します。

UNIXファイルシステムのバックアップの監視

バックアップ処理とデータ保護処理の進捗状況を監視する方法について説明します。

UNIXファイルシステムのバックアップ処理の監視

SnapCenterの[Jobs]ページを使用して、各種バックアップ処理の進捗状況を監視できます。進捗状況をチェックして、インストールが完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。アイコンの意味については、それぞれの説明をご覧ください。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*ジョブ*をクリックします。
3. [Jobs]ページで、次の手順を実行します。
 - a. をクリックして、 リストの内容をバックアップ処理だけに絞り込みます。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*バックアップ*を選択します。
 - d. *ステータス*ドロップダウンから、バックアップのステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. バックアップ ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。



バックアップジョブのステータスは  ジョブの詳細をクリックすると、バックアップ操作の子タスクの一部がまだ進行中であるか、警告サインが付いていることがわかる場合があります。

5. ジョブの詳細ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

[Activity]ペインでデータ保護処理を監視

[Activity]ペインには、最後に実行された5つの処理が表示されます。また[Activity]ペインには、処理が開始された日次と処理のステータスが表示されます。

[Activity]ペインには、バックアップ、リストア、クローニング、スケジュールされたバックアップの各処理に関する情報が表示されます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. クリック  アクティビティ ペインで、最新の 5 つの操作を表示します。

いずれかの操作をクリックすると、*ジョブの詳細*ページに操作の詳細が表示されます。

[Topology] ページで保護されている UNIX ファイルシステムの表示

リソースのバックアップ、リストア、またはクローニングを準備する際に、プライマリストレージとセカンダリ ストレージ上のすべてのバックアップ、リストアしたファイルシステム、およびクローンの図を表示すると役に立ちます。

このタスクについて

[Topology] ページでは、選択したリソースまたはリソース グループに使用できるバックアップ、リストアしたファイルシステム、およびクローンをすべて表示できます。これらのバックアップ、リストアしたファイルシステム、およびクローンの詳細を参照し、対象を選択してデータ保護処理を実行できます。

プライマリ ストレージまたはセカンダリ ストレージ（ミラー コピーまたはバックアップ コピー）にバックアップとクローンがあるかどうかは、[Manage Copies] ビューの次のアイコンで確認できます。

-  プライマリ ストレージで使用可能なバックアップとクローンの数を表示します。
-  SnapMirrorテクノロジーを使用してセカンダリ ストレージにミラーリングされているバックアップとクローンの数を表示します。
-  SnapVaultテクノロジーを使用してセカンダリ ストレージに複製されたバックアップとクローンの数を表示します。

表示されるバックアップの数には、セカンダリ ストレージから削除されたバックアップも含まれます。たとえば、バックアップを4個保持するポリシーを使用してバックアップを6個作成した場合、バックアップの数は6個と表示されます。



mirror-vaultタイプのボリュームにあるバージョンに依存しないミラーのバックアップのクローンはトポロジ ビューに表示されますが、トポロジ ビューのミラー バックアップの数にはバージョンに依存しないバックアップは含まれません。

SnapMirrorアクティブ同期 (当初はSnapMirror Business Continuity [SM-BC] としてリリース) としてセカンダリ関係がある場合は、次の追加アイコンが表示されます。

-  レプリカサイトが稼働しています。
-  レプリカサイトはダウンしています。



セカンダリ ミラーまたはボールド関係が再確立されていません。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストからリソースまたはリソース グループを選択します。
3. リソースの詳細ビューまたはリソース グループの詳細ビューで、リソースを選択します。

リソースが保護されている場合は、選択したリソースの[Topology]ページが表示されます。

4. [Summary Card]で、プライマリ ストレージとセカンダリ ストレージ上にあるバックアップとクローンの数の概要を確認します。

[Summary Card]セクションには、バックアップとクローンの総数が表示されます。

更新 ボタンをクリックすると、ストレージのクエリが開始され、正確な数が表示されます。

SnapLock対応バックアップが取得された場合、[更新] ボタンをクリックすると、ONTAPから取得されたプライマリおよびセカンダリSnapLockの有効期限が更新されます。週次スケジュールでも、ONTAPから取得したプライマリおよびセカンダリのSnapLock有効期限が更新されます。

ファイルシステムが複数のボリュームに分散している場合、バックアップのSnapLock有効期限は、ボリューム内のSnapshotに設定されている最長のSnapLock有効期限になります。最長のSnapLock有効期限はONTAPから取得されます。

SnapMirrorアクティブ同期の場合、[更新] ボタンをクリックすると、プライマリ サイトとレプリカ サイトの両方に対してONTAPを照会してSnapCenterバックアップ インベントリが更新されます。週次スケジュールでも、SnapMirrorアクティブ同期関係を含むすべてのデータベースに対してこの処理が実行されます。

- SnapMirrorアクティブ同期とONTAP（バージョン9.14.1のみ）では、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップの関係については、フェイルオーバー後に手動で設定する必要があります。ONTAP 9.15.1以降は、新しいプライマリ デスティネーションに対する非同期ミラーまたは非同期ミラー バックアップが、自動的に設定されます。
- フェイルオーバーが完了したら、SnapCenterがフェイルオーバーを認識できるようにバックアップを作成する必要があります。バックアップが作成された後にのみ、「更新」をクリックできます。

5. 「コピーの管理」ビューで、プライマリ ストレージまたはセカンダリ ストレージから バックアップ または クローン をクリックして、バックアップまたはクローンの詳細を表示します。

バックアップとクローンの詳細が表形式で表示されます。

6. 表でバックアップを選択し、データ保護アイコンをクリックして、リストア、クローニング、削除の各処理を実行します。



セカンダリ ストレージ上のバックアップは、名前変更または削除できません。

7. クローンを削除する場合は、表でクローンを選択し、 をクリックします。

プライマリ ストレージのバックアップとクローンの例



UNIXファイルシステムのリストアとリカバリ

UNIXファイルシステムのリストア

データ損失が発生した場合は、SnapCenterを使用してUNIXファイルシステムをリストアできます。

このタスクについて

- 次の各コマンドを実行して、SnapCenter Serverとの接続を確立し、バックアップをリストしてその情報を取得し、バックアップをリストアする必要があります。

コマンドで使用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、["SnapCenterソフトウェア コマンド リファレンス ガイド"](#)。

- SnapMirrorアクティブ同期でリストア処理を実行するには、プライマリの場所からバックアップを選択する必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [パス] または [リソース グループ] のいずれかを選択します。

3. 詳細ビューまたはリソース グループの詳細ビューでファイルシステムを選択します。

トポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたは複製された) ストレージ システムから [バックアップ] を選択します。

5. 表からバックアップを選択し、*をクリックします。  *。

6. [Restore Scope] ページ：

- NFS ファイル システムの場合、デフォルトで 接続とコピー 復元が選択されます。 *ボリュームの復元*または*高速復元*を選択することもできます。
- NFS以外のファイルシステムの場合は、レイアウトに応じてリストア範囲が選択されます。

ファイルシステムのタイプとレイアウトによっては、バックアップ後に作成された新しいファイルをリストア後に使用できない場合があります。

7. [PreOps] ページで、リストア ジョブの実行前に実行するリストア前の処理のコマンドを入力します。

8. [PostOps] ページで、リストア ジョブの実行後に実行するリストア後の処理のコマンドを入力します。



プラグイン ホスト上の `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config` パスにあるコマンド リストにコマンドが存在するかどうかを確認する必要があります。

9. [通知] ページの [電子メール設定] ドロップダウン リストから、電子メール通知を送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。実行された復元操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択する必要があります。



Eメール通知を利用する場合は、GUIまたはPowerShellコマンドSet-SmSmtServerを使用して、SMTPサーバの詳細を指定しておく必要があります。

10. 概要を確認し、[完了] をクリックします。



リストア処理が失敗した場合のロールバックはサポートされていません。



ボリューム グループ上にあるファイルシステムをリストアしても、ファイルシステム上の古いコンテンツは削除されません。クローニングされたファイルシステムのコンテンツだけがソース ファイルシステムにコピーされます。これは、ボリューム グループに複数のファイルシステムがあり、デフォルトのNFSファイルシステムがリストアされる場合に該当します。

11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

UNIXファイルシステムのリストア処理の監視

[Job] ページを使用して、SnapCenterの各リストア処理の進捗状況を監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうか

かを確認できます。

タスク概要

リストア後の状態によって、リストア処理後のリソースの状況と、追加で実行できるリストア操作がわかります。

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  でリストをフィルタリングし、リストア処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*復元*を選択します。
 - d. *ステータス*ドロップダウンリストから、復元ステータスを選択します。
 - e. 正常に完了した操作を表示するには、[適用] をクリックします。
4. 復元ジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
5. *ジョブの詳細*ページで、*ログの表示*をクリックします。

ログを表示 ボタンをクリックすると、選択した操作の詳細なログが表示されます。

UNIXファイルシステムのクローニング

UNIXファイルシステムのバックアップのクローニング

SnapCenterを使用すると、ファイルシステムのバックアップを使用してUNIXファイルシステムをクローニングできます。

開始する前に

- `/opt/NetApp/snapcenter/scc/etc` にある `agent.properties` ファイルで `SKIP_FSTAB_UPDATE` の値を **true** に設定することで、fstab ファイルの更新をスキップできます。
- `/opt/NetApp/snapcenter/scc/etc` にある `agent.properties` ファイルで

`USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT` の値を **true** に設定することで、静的なクローン ボリューム名とジャンクション パスを設定できます。ファイルを更新した後、次のコマンドを実行して SnapCenter プラグイン作成者サービスを再起動する必要があります。

```
/opt/NetApp/snapcenter/scc/bin/scc restart。
```

例: このプロパティがない場合、クローン ボリューム名とジャンクション パスは `<Source_volume_name>_Clone_<Timestamp>` のようになりますが、このプロパティを使用すると `<Source_volume_name>_Clone_<Clone_Name>` になります。

これにより名前が一定に保たれ、SnapCenterによってfstabが更新されるのが好ましくない場合に、fstab ファイルを手動で更新できるようになります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [パス] または [リソース グループ] のいずれかを選択します。
3. 詳細ビューまたはリソース グループの詳細ビューでファイルシステムを選択します。

トポロジ ページが表示されます。

4. [Manage Copies]ビューで、ローカル コピー（プライマリ）、ミラー コピー（セカンダリ）、バックアップ コピー（セカンダリ）のいずれかのバックアップを選択します。
5. 表からバックアップを選択し、*をクリックします。  *。
6. [Location]ページで、次の操作を実行します。

フィールド	操作
Clone server	ソース ホストがデフォルトで入力されています。
Clone mount point	ファイルシステムをマウントするパスを指定します。

7. [Scripts]ページで、次の手順を実行します。
 - a. クローニング処理の前後に実行するプリコマンドやポストコマンドを入力します。



`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config` パスからプラグイン ホスト上で使用可能なコマンド リストにコマンドが存在するかどうかを確認する必要があります。

8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。実行されたクローン操作のレポートを添付する場合は、「ジョブ レポートの添付」を選択します。



Eメール通知を利用する場合は、GUIまたはPowerShellのSet-SmSmtptServerコマンドを使用して、SMTPサーバの詳細を指定しておく必要があります。

9. 概要を確認し、[完了] をクリックします。
10. モニター > ジョブ をクリックして、操作の進行状況を監視します。

クローンのスプリット

SnapCenterを使用して、クローン リソースを親リソースからスプリットできます。スプリットされたクローンは親リソースから独立します。

タスク概要

- 中間クローンではクローン スプリット処理を実行できません。

たとえば、データベース バックアップからクローン1を作成したあとで、クローン1のバックアップを作成し、そのバックアップ（クローン2）をクローニングできます。クローン2を作成すると、クローン1は中間クローンになり、クローン1ではクローン スプリット処理を実行できなくなります。ただし、クローン2に対してはクローン スプリット処理を実行できます。

クローン2をスプリットすると、クローン1は中間クローンではなくなるため、クローン1に対してクローン スプリット処理を実行できるようになります。

- クローンをスプリットすると、そのクローンのバックアップ コピーとクローン ジョブが削除されます。
- FlexCloneボリューム分割操作の詳細については、以下を参照してください。 ["親ボリュームからFlexCloneボリュームのスプリット"](#)。
- ストレージ システム上のボリュームまたはアグリゲートがオンラインであることを確認します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. *リソース*ページで、表示リストから適切なオプションを選択します。

オプション	説明
データベース アプリケーションの場合	表示リストから*データベース*を選択します。
ファイルシステムの場合	表示リストから*パス*を選択します。

3. リストから適切なリソースを選択します。

リソースのトポロジ ページが表示されます。

4. *コピーの管理*ビューから、クローンされたリソース（データベースやLUNなど）を選択し、*をクリックします。  *。
5. 分割するクローンの推定サイズとアグリゲート上で必要な空き容量を確認し、[開始] をクリックします。
6. モニター > ジョブ をクリックして、操作の進行状況を監視します。

SMCoreサービスが再起動されると、クローン スプリット処理は応答を停止します。Stop-SmJobコマンドレットを実行してクローン スプリット処理を停止してから、クローン スプリット処理を再試行してください。

クローンが分割されているかどうかを確認するためのポーリング時間を長くしたり短くしたりする場合は、`SMCoreServiceHost.exe.config` ファイルの `CloneSplitStatusCheckPollTime` パラメータの値を変更して、SMCore がクローン分割操作のステータスをポーリングする時間間隔を設定できます。値はミリ秒単位で、デフォルト値は5分です。

例えば：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

バックアップ、リストア、または別のクローン スプリットが実行中の場合、クローン スプリットの開始処理は失敗します。クローン スプリット処理を再開するのは、実行中の処理が完了してからにしてください。

関連情報

["アグリゲートが存在しないためにSnapCenterのクローニングや検証が失敗する"](#)

UNIXファイルシステムのクローニング処理の監視

SnapCenterのクローニング処理の進捗状況を、[Jobs]ページで監視できます。処理の進捗状況をチェックして、処理が完了するタイミングや問題が発生していないかどうかを確認できます。

タスク概要

[Jobs]ページでは、次のアイコンで処理の状態が示されます。

-  進行中
-  正常に完了しました
-  失敗した
-  警告付きで完了したか、警告のため開始できませんでした
-  キューに登録
-  キャンセル

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. *モニター*ページで、*ジョブ*をクリックします。
3. ジョブ ページで、次の手順を実行します。
 - a. をクリックし  てリストをフィルタリングし、クローニング処理のみを表示します。
 - b. 開始日と終了日を指定します。
 - c. *タイプ*ドロップダウンリストから*クローン*を選択します。
 - d. *ステータス*ドロップダウンリストからクローンのステータスを選択します。

- e. 正常に完了した操作を表示するには、[適用] をクリックします。
- 4. クローンジョブを選択し、[詳細] をクリックしてジョブの詳細を表示します。
- 5. ジョブの詳細ページで、*ログの表示*をクリックします。

Azure NetApp Filesで実行されているアプリケーションの保護

Azure NetApp Filesで実行されているアプリケーションの保護

SnapCenter は、Azure NetApp Files上にある Oracle、SQL、SAP HANA などのアプリケーションの保護をサポートしています。6.0.1 リリース以降、SnapCenter は、長期的なリカバリ、アーカイブ、コンプライアンスのための完全に管理されたバックアップソリューションを提供することで、Azure NetApp Filesのデータ保護機能を拡張する Azure NetApp Filesバックアップ機能をサポートします。

Azure NetApp Files は、長期のバックアップ保持には高額になる可能性があるプレミアム ストレージ ソリューションです。コストを最適化するには、Azure NetApp Filesストレージから Azure オブジェクト ストアにバックアップを移動できます。SnapCenter 6.0.1 以降では、Azure NetApp Filesにあるアプリケーションを Azure Blob Storage (オブジェクト ストア) にバックアップおよびクローンできます。データのコピーを 2 つ保持できます。短期的な回復のためにボリューム スナップショットのコピーを Azure NetApp Filesストレージに保持し、長期的な回復のために別のコピーを Azure Blob Storage に保持します。

Azure NetApp Filesバックアップのポリシーが有効になっていてリソースに関連付けられている場合、SnapCenter はボリューム スナップショットの作成と Azure Blob Storage へのバックアップを処理します。SnapCenter はバックアップ ボールトを作成し、ボリュームのバックアップを有効にします。ボリュームのバックアップを有効にしている場合、SnapCenter は既存のボールトを利用します。

制限事項

- FAS、ASA、またはAFF ONTAPおよびAmazon FSx for NetApp ONTAPストレージ システムのオブジェクト ストレージ機能はサポートされていません。
- Oracle および SAP HANA のマウントおよびカタログ ワークフローは、オブジェクト ストレージ バックアップではサポートされていませんが、スナップショットではサポートされています。
- Oracle PDB クローンはオブジェクト ストレージ バックアップではサポートされていませんが、スナップショットではサポートされています。
- オブジェクト ストレージからのバックアップ検証、REST API サポート、オブジェクト ストレージからのクローン ライフサイクル管理、およびオブジェクト ストレージ バックアップのレポート機能はサポートされていません。
- Azure Blob Storage 上のバックアップから Azure NetApp Filesへの復元はサポートされていません。代わりにクローン オプションを使用することもできます。
- クローン分割はサポートされていません。

SnapCenterのインストールとクレデンシャルの作成

Azure仮想マシンへのSnapCenterのインストール

NetAppサポート サイトからSnapCenterソフトウェアをダウンロードし、Azure仮想マシンにインストールできます。

開始する前に

- Azure Windows仮想マシンがSnapCenter Serverのインストール要件を満たしていることを確認します。詳細については、"[SnapCenter Server をインストールするための要件](#)"。
- Azure NetApp Filesを初めてご利用になり、既存のNetAppアカウントをお持ちでない場合は、SnapCenter ソフトウェアにアクセスできるように必ず登録を済ませてください。詳細については、"[SnapCenterソフトウェアにアクセスするための登録](#)"。

手順

1. SnapCenter Serverのインストールパッケージを以下からダウンロードします。 "[NetAppサポート サイト](#)"。
2. ダウンロードした.exeファイルをダブルクリックして、SnapCenter Serverのインストールを開始します。

インストールを開始すると、すべての事前確認が実行されます。最小要件を満たしていない場合は、対応するエラーまたは警告メッセージが表示されます。警告メッセージは無視してインストールを続行できますが、エラーは修正する必要があります。

3. SnapCenter Serverのインストールに必要な入力済みの値を確認し、必要に応じて変更します。

MySQL Serverリポジトリ データベースのパスワードを指定する必要はありません。SnapCenter Serverのインストール時には、パスワードが自動生成されます。



リポジトリ データベースのカスタム パスに特殊文字「%」を使用することはできません。パスに「%」が含まれているとインストールは失敗します。

4. *今すぐインストール*をクリックします。

無効な値を指定すると、対応するエラー メッセージが表示されます。値を再入力してからインストールを開始してください。



*キャンセル*ボタンをクリックすると、実行中のステップが完了し、ロールバック操作が開始されます。SnapCenter Serverはホストから完全に削除されます。

ただし、「SnapCenter Server サイトの再起動」または「SnapCenter Server の起動を待機中」の操作の実行中に [キャンセル] をクリックすると、操作はキャンセルされずにインストールが続行されます。

製品の登録とサポートの有効化

NetAppを初めてご利用になり、既存のNetAppアカウントをお持ちでない場合は、製品を登録してサポートを有効にする必要があります。

手順

1. SnapCenterをインストールした後、*ヘルプ > バージョン情報*に移動します。
2. [SnapCenter について] ダイアログ ボックスで、971 で始まる 20 桁の番号であるSnapCenterインスタンスをメモします。
3. クリック <https://register.netapp.com>。
4. 私はNetAppの登録顧客ではありません をクリックします。

5. ご自身の情報を指定して、登録します。
6. [NetApp Reference SN]フィールドは空白のままにします。
7. 製品ラインドロップダウンから* SnapCenter*を選択します。
8. 課金プロバイダを選択します。
9. 20桁のSnapCenterインスタンスIDを入力します。
10. *送信*をクリックします。

SnapCenterでのAzureクレデンシャルの作成

Azure NetAppアカウントにアクセスするには、SnapCenterでAzureクレデンシャルを作成する必要があります。

開始する前に

- Azure でサービス プリンシパルを作成したことを確認します。
- 使用可能なサービス プリンシパルに関連付けられたテナント ID、クライアント ID、および秘密キーがあることを確認します。
 - テナント ID は、Azure Portal の Entra ID の概要ページで確認できます。
 - クライアント ID は、エンタープライズ アプリ/サービス プリンシパルのアプリケーション ID と呼ばれます。これは、SnapCenterのサービス プリンシパルとして機能するように作成したエンタープライズ アプリケーションの概要ページの Azure Portal にあります。
 - クライアント秘密キーは秘密値とも呼ばれます。このクライアント シークレットは、Azure Portal の Entra ID の下の アプリ登録 に移動することで作成できます。作成したエンタープライズ アプリを選択した後、証明書とシークレット、新しいクライアント シークレット に移動します。



秘密値にアクセスできるのは作成時のみです。後からアクセスすることはできません。

- サービス プリンシパルに権限を付与する必要があります。共同作成者の役割により、サービス プリンシパルは Azure で必要なアクションを実行できるようになります。これは、サブスクリプション ページ内のアクセス制御 (IAM) ページから付与できます。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[資格情報]をクリックします。
3. *新規*をクリックします。
4. [Credential]ページで、クレデンシャルの作成に必要な次の情報を指定します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。
Authentication Mode	ドロップダウン リストから Azure 資格情報 を選択します。

フィールド	操作
テナントID	テナントIDを入力します。
クライアントID	クライアントIDを入力します。
Client Secret Key	クライアント シークレット キーを入力します。

5. [OK]をクリックします。

Azureストレージ アカウントの設定

SnapCenterでAzureストレージ アカウントを設定する必要があります。

Azureストレージ アカウントには、サブスクリプションID、Azureクレデンシャル、およびAzure NetAppアカウントの詳細が含まれます。



Azure NetApp Filesには、Standardライセンスと容量ベースライセンスは必要ありません。

手順

1. 左側のナビゲーション ペインで、[ストレージ システム] をクリックします。
2. [ストレージ システム] ページで、* Azure NetApp Files* を選択し、新規 をクリックします。
3. クレデンシャル、サブスクリプションID、およびNetAppアカウントをそれぞれのドロップダウン リストから選択します。
4. *送信*をクリックします。

プラグイン ホストに追加するクレデンシャルの作成

SnapCenterは、クレデンシャルを使用してSnapCenterの処理を実行するユーザを認証します。

SnapCenterプラグインのインストールに使用するクレデンシャルと、データ保護処理に使用する追加のクレデンシャルをそれぞれ作成する必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[資格情報]をクリックします。
3. *新規*をクリックします。
4. [Credential]ページで、クレデンシャルの作成に必要な次の情報を指定します。

フィールド	操作
資格情報名	クレデンシャルの名前を入力します。

フィールド	操作
Authentication Mode	ドロップダウン リストから認証モードを選択します。
Authentication Type	パスワード ベース または SSH キー ベース (Linux ホストのみ) を選択します。
ユーザー名	ユーザ名を指定します。
パスワード	パスワード ベースの認証を選択した場合は、パスワードを指定します。
SSH Private Key	SSHキー ベースの認証を選択した場合は、秘密鍵を指定します。
Use sudo privileges	root以外のユーザに対してクレデンシャルを作成する場合は、[Use sudo privileges]チェック ボックスをオンにします。  これは、Linuxユーザにのみ適用されます。

5. [OK]をクリックします。

SAP HANAデータベースの保護

ホストの追加とSnapCenter Plug-in for SAP HANA Databaseのインストール

SnapCenterの[Add Host]ページを使用してホストを追加し、プラグイン パッケージをインストールする必要があります。プラグインは、自動的にリモート ホストにインストールされます。

開始する前に

- この処理は、SnapCenter Adminロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。
- 一元化されたホストにインストールする場合は、SAP HANAクライアント ソフトウェアがそのホストにインストールされていることを確認し、HDB SQLクエリをリモートで実行できるようにSAP HANAデータベース ホストで必要なポートを開きます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. *管理対象ホスト*タブが選択されていることを確認します。

3. *[追加]*をクリックします。
4. [Hosts]ページで、次の操作を実行します。
 - a. [Host Type]フィールドで、ホスト タイプを選択します。
 - b. [Host name]フィールドに、ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。
 - c. [Credentials]フィールドに、作成したクレデンシャルを入力します。
5. [Select Plug-ins to Install]セクションで、インストールするプラグインを選択します。
6. (オプション) [その他のオプション] をクリックして詳細を指定します。
7. *送信*をクリックします。
8. ホスト タイプが Linux の場合は、フィンガープリントを確認し、[確認して送信] をクリックします。

クラスタ セットアップでは、クラスタ内の各ノードのフィンガープリントを検証する必要があります。
9. インストールの進捗状況を監視します。

SAP HANAデータベースの追加

SAP HANAデータベースは手動で追加する必要があります。

タスク概要

一元化されたサーバにプラグインがインストールされている場合は、リソースを手動で追加する必要があります。HANAデータベース ホストにSAP HANAプラグインがインストールされている場合は、HANAシステムが自動的に検出されます。



自動検出はHANAマルチホスト構成ではサポートされていません。追加するには一元化されたプラグインのみを使用する必要があります。

手順

1. 左側のナビゲーション ペインで、ドロップダウン リストから SAP HANA データベース用のSnapCenter プラグインを選択し、リソース をクリックします。
2. リソース ページで、**SAP HANA** データベースの追加 をクリックします。
3. [Provide Resource Details]ページで、次の操作を実行します。
 - a. リソース タイプとして、単一のコンテナ、マルチテナント データベース コンテナ、またはデータ ボリューム以外のボリュームのいずれかを入力します。
 - b. SAP HANAシステムの名前を入力します。
 - c. システムID（SID）を入力します。
 - d. プラグイン ホストを選択します。
 - e. SAP HANAシステムに接続するためのキーを入力します。
 - f. [HDB Secure User Store Key]でキーを設定するユーザの名前を入力します。
4. [ストレージ フットプリントの提供] ページで、ストレージの種類として [* Azure NetApp Files*] を選択します。
 - a. Azure NetAppアカウントを選択します。

- b. 容量プールと関連ボリュームを選択します。
 - c. *保存*をクリックします。
5. 概要を確認し、[完了] をクリックします。

SAP HANAデータベースのバックアップ ポリシーの作成

SnapCenterを使用してSAP HANAデータベースのリソースをバックアップする前に、バックアップ対象のリソースまたはリソース グループのバックアップ ポリシーを作成する必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定] ページで、[ポリシー] をクリックします。
3. *新規* をクリックします。
4. [Name] ページで、ポリシーの名前と説明を入力します。
5. ポリシー タイプ ページで、次の手順を実行します。
 - a. ストレージの種類として * Azure NetApp Files* を選択します。
 - b. データベースの整合性チェックを実行する場合は、「ファイルベース」を選択します。
 - c. スナップショット テクノロジーを使用してバックアップを作成する場合は、「スナップショット ベース」を選択します。
6. スナップショットとバックアップ ページで、次の手順を実行します。
 - a. スケジュールされたバックアップの頻度を選択します。
 - b. 保持設定を指定します。
 - c. Azure NetApp Filesバックアップを有効にする場合は、[バックアップを有効にする] を選択し、保持設定を指定します。
7. 概要を確認し、[完了] をクリックします。

リソース グループの作成とSAP HANAバックアップ ポリシーの適用

リソース グループはコンテナであり、バックアップして保護するリソースをここに追加する必要があります。

リソース グループを使用することで、特定のアプリケーションに関連するすべてのデータを同時にバックアップできます。リソース グループはいずれのデータ保護ジョブにも必要になります。リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義することも必要です。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。

フィールド	操作
Name	リソース グループの名前を入力します。
Tags	リソース グループを検索しやすくするために、ラベルを入力します。
Use custom name format for Snapshot copy	Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

- [リソース] ページで、[ホスト] ドロップダウン リストからホスト名を選択し、[リソース タイプ] ドロップダウン リストからリソース タイプを選択します。
- *利用可能なリソース*セクションからリソースを選択し、右矢印をクリックして*選択したリソース*セクションに移動します。
- [Policies] ページで、次の手順を実行します。
 - ドロップダウン リストから1つ以上のポリシーを選択します。
 - スケジュールの設定列で*をクリックします。  * 設定するポリシーの。
 - ポリシー *policy_name* のスケジュールの追加ダイアログ ボックスでスケジュールを構成し、[OK] をクリックします。
- 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。
- 概要を確認し、[完了] をクリックします。

Azure NetApp Filesで実行されているSAP HANAデータベースのバックアップ

どのリソース グループにもまだ含まれていないリソースは、[Resources] ページからバックアップすることができます。

手順

- 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
- リソース ページで、リソース タイプに基づいて 表示 ドロップダウン リストからリソースをフィルターします。
- バックアップするリソースを選択します。
- [リソース] ページで、[スナップショット コピーにカスタム名形式を使用する] を選択し、スナップショット名に使用するカスタム名形式を入力します。
- [Application Settings] ページで、次の操作を実行します。
 - 追加のバックアップ オプションを設定するには、[バックアップ] 矢印を選択します。
 - *スクリプト*矢印を選択して、静止、スナップショット、および静止解除操作の事前および事後コマンドを実行します。
 - *カスタム構成*矢印を選択し、このリソースを使用するすべてのジョブに必要なカスタム値のペアを入力します。

- d. スナップショットを作成するには、*スナップショット コピー ツール> ファイル システムの整合性のないSnapCenter* を選択します。

ファイル システムの整合性 オプションは、Windows ホスト上で実行されているアプリケーションにのみ適用されます。

6. [Policies]ページで、次の手順を実行します。

- a. ドロップダウン リストから1つ以上のポリシーを選択します。
- b. を選択  スケジュールを構成するポリシーの [スケジュールの構成] 列で、
- c. ポリシー *policy_name* のスケジュールの追加 ダイアログ ボックスでスケジュールを構成し、[OK] を選択します。

policy_name は選択したポリシーの名前です。

7. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP は、設定> グローバル設定 でも設定する必要があります。

8. 概要を確認し、[完了] を選択します。

9. *今すぐバックアップ*を選択します。

10. [Backup]ページで次の手順を実行します。

- a. リソースに複数のポリシーが関連付けられている場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

11. *バックアップ*を選択します。

12. モニター> ジョブ をクリックして、操作の進行状況を監視します。

SAP HANAリソース グループのバックアップ

リソース グループは、ホスト上のリソースの集まりです。リソース グループのバックアップ処理は、リソース グループに定義されているすべてのリソースを対象に実行されます。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。
3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] を選択します。
4. [Backup]ページで次の手順を実行します。
 - a. リソース グループに複数のポリシーが関連付けられている場合は、[ポリシー] ドロップダウン リスト

から、バックアップに使用するポリシーを選択します。

オンデマンド バックアップ用に選択したポリシーがバックアップ スケジュールに関連付けられている場合、オンデマンド バックアップは、スケジュール タイプの保持設定に基づいて保持されます。

b. *バックアップ*を選択します。

5. モニター > ジョブ を選択して、操作の進行状況を監視します。

SAP HANAデータベースのリストアとリカバリ

バックアップからデータをリストアおよびリカバリできます。

タスク概要

自動検出された HANA システムでは、完全なリソース オプションが選択されている場合、単一ファイル スナップショット復元テクノロジーを使用して復元が実行されます。高速復元 チェックボックスが選択されている場合は、ボリューム復元テクノロジーが使用されます。

手動で追加したリソースには、常にボリューム リバート テクノロジーが使用されます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。
3. リソースを選択するか、リソース グループを選択してそのグループ内のリソースを選択します。
4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたはボルト化された) ストレージ システムから [バックアップ] を選択します。
5. プライマリバックアップテーブルで、復元するバックアップを選択し、*をクリックします。  *。
6. 復元範囲ページで、*完全なリソース*を選択します。

SAP HANAデータベースのすべての設定済みデータ ボリュームがリストアされます。

7. 自動検出されたHANAシステムの場合は、[Recovery scope]ページで次の操作を実行します。
 - a. 可能な限り現在の時刻に近い状態に復元したい場合は、「最新の状態に復元」を選択します。
 - b. 指定した時点に回復する場合は、「特定の時点に回復」を選択します。
 - c. 特定のデータ バックアップに復元する場合は、[指定されたデータ バックアップに復元] を選択します。
 - d. 今すぐ回復したくない場合は、「回復なし」を選択します。
 - e. ログ バックアップの場所を指定します。
 - f. バックアップ カタログの場所を指定します。
8. [Pre ops]ページで、リストア ジョブの実行前に実行するリストア前の処理とアンマウントのコマンドを入力します。
9. [Post ops]ページで、リストア ジョブの実行後に実行するマウントとリストア後の処理のコマンドを入力します。

10. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

また、送信者と受信者のEメール アドレス、およびEメールの件名を指定する必要があります。SMTP は、[設定]>[グローバル設定] ページでも設定する必要があります。

11. 概要を確認し、[完了] をクリックします。
12. モニター>ジョブ をクリックして、操作の進行状況を監視します。

SAP HANAデータベースのバックアップのクローニング

SnapCenter を使用すると、データベースのバックアップを使用して SAP HANA データベースのクローンを作成できます。作成されるクローンはシック クローンであり、親容量プール上に作成されます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、リソース タイプに基づいて [表示] ドロップダウン リストからリソースをフィルターします。
3. リソースまたはリソース グループを選択します。
4. [コピーの管理] ビューで、プライマリ ストレージ システムから [バックアップ] を選択します。
5. 表からデータバックアップを選択し、クリックします。 .
6. [Location] ページで、次の操作を実行します。
 - a. クローンHANAシステムを管理するためのSAP HANAプラグインがインストールされているホストを選択します。

集中型プラグイン ホストまたは HANA システム ホストにすることができます。



HANA プラグインが、他のホスト上の HANA データベースを管理する集中ホストにインストールされている場合、クローンを作成または削除するときに、ターゲット サーバーが集中ホストであるため、SnapCenter はホスト側の操作 (ファイルシステムのマウントまたはアンマウント) を意図的にスキップします。マウントおよびアンマウント操作を実行するには、カスタムのクローン前スクリプトまたはクローン後スクリプトを使用する必要があります。

- a. 既存のバックアップからクローニングするSAP HANA SIDを入力します。
- b. クローン ボリュームをエクスポートするホスト名またはIPアドレスを入力します。
- c. SAP HANAデータベースANFボリュームが手動QoS容量プールに設定されている場合は、クローン ボリュームのQoSを指定します。

クローン ボリュームにQoSが指定されていない場合は、ソース ボリュームのQoSが使用されます。自動QoS容量プールを使用している場合、指定したQoS値は無視されます。

7. [Scripts] ページで、次の手順を実行します。
 - a. クローニング処理の前後に実行するプリコマンドやポストコマンドを入力します。

- b. ホストにファイルシステムをマウントするには、mountコマンドを入力します。

ソースHANAシステムが自動検出され、クローン ターゲット ホスト プラグインがSAP HANAホストにインストールされている場合、SnapCenterはクローン ターゲット ホスト上の既存のHANAデータ ボリュームを自動的にアンマウントし、新しくクローニングされたHANAデータ ボリュームをマウントします。

8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。
9. 概要を確認し、[完了] をクリックします。
10. モニター > ジョブ をクリックして、操作の進行状況を監視します。



ANFクローンはすでに、選択したSnapshotから作成された独立したボリュームであるため、ANFクローンではクローン スプリットが無効になります。

Microsoft SQL Serverデータベースの保護

ホストの追加とSnapCenter Plug-in for SQL Server Databaseのインストール

SnapCenterは、Azure NetApp Files上のSMB共有にあるSQLインスタンスのデータ保護をサポートしています。スタンドアロン構成と可用性グループ（AG）構成がサポートされています。

SnapCenterの[Add Host]ページを使用してホストを追加し、プラグイン パッケージをインストールする必要があります。プラグインは、自動的にリモート ホストにインストールされます。

開始する前に

- この処理は、SnapCenter Adminロールなど、プラグインのインストールとアンインストールの権限のあるロールが割り当てられているユーザが実行する必要があります。
- Windowsホストにプラグインをインストールする際、組み込みでないクレデンシャルを指定する場合や、ユーザがローカル ワークグループに属している場合は、ホストのUACを無効にする必要があります。

手順

1. 左側のナビゲーション ペインで、[ホスト] を選択します。
2. 上部の*管理対象ホスト*タブが選択されていることを確認します。
3. *追加*を選択します。
4. [Hosts]ページで次の操作を実行します。
 - a. [Host Type]フィールドで、ホスト タイプを選択します。
 - b. [Host name]フィールドに、ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。
 - c. [Credentials]フィールドに、作成したクレデンシャルを入力します。
5. *インストールするプラグインの選択*セクションで、インストールするプラグインを選択します。
6. (オプション) [その他のオプション] をクリックして詳細を指定します。
7. *送信*を選択します。

8. ログ ディレクトリの構成 を選択し、ホスト ログ ディレクトリの構成ページで、ホスト ログ ディレクトリの SMB パスを入力して、保存 をクリックします。
9. [送信] をクリックして、インストールの進行状況を監視します。

SQL Serverデータベースのバックアップ ポリシーの作成

SnapCenterを使用してSQL Serverリソースをバックアップする前に、リソースまたはリソース グループのバックアップ ポリシーを作成することができます。また、リソース グループの作成時や単一のリソースのバックアップ時にバックアップ ポリシーを作成することも可能です。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[ポリシー]をクリックします。
3. *新規*をクリックします。
4. [Name]ページで、ポリシーの名前と説明を入力します。
5. ポリシー タイプ ページで、次の手順を実行します。
 - a. ストレージの種類として * Azure NetApp Files* を選択します。
 - b. バックアップ タイプを選択します。
 - i. データベース ファイルとトランザクション ログをバックアップする場合は、完全バックアップとログ バックアップ を選択します。
 - ii. データベース ファイルのみをバックアップする場合は、[完全バックアップ] を選択します。
 - iii. トランザクション ログのみをバックアップする場合は、[ログ バックアップ] を選択します。
 - iv. 別のアプリケーションを使用してリソースをバックアップする場合は、「コピーのみのバックアップ」を選択します。
 - c. [Availability Group Settings]セクションで、次の操作を実行します。
 - i. レプリカのみにバックアップする場合は、[Backup on preferred backup replica]を選択します。
 - ii. バックアップするプライマリまたはセカンダリのAGレプリカを選択します。
 - iii. バックアップの優先順位を選択します。
6. スナップショットとバックアップ ページで、次の手順を実行します。
 - a. スケジュールされたバックアップの頻度を選択します。
 - b. 選択したバックアップの種類に応じて保持設定を指定します。
 - c. Azure NetApp Filesバックアップを有効にする場合は、[バックアップを有効にする] を選択し、保持設定を指定します。
7. [Verification]ページで、次の手順を実行します。
 - a. [Run verification for following backup schedules]セクションで、実行頻度を選択します。
 - b. [Database consistency check options]セクションで、次の操作を実行します。
 - i. 整合性チェックをデータベースの物理構造に制限し、破損したページ、チェックサム障害、およびデータベースに影響する一般的なハードウェア障害を検出するには、[整合性構造をデータベ

スの物理構造に制限する (PHYSICAL_ONLY)] を選択します。

- ii. すべての情報メッセージを抑制するには、すべての情報メッセージを抑制 (**NO_INFOMSGS**) を選択します。

このオプションはデフォルトで選択されています。

- iii. オブジェクトごとに報告されたすべてのエラーを表示するには、オブジェクトごとに報告されたすべてのエラー メッセージを表示する (**ALL_ERRORMSGs**) を選択します。
- iv. 非クラスター化インデックスをチェックしない場合は、[非クラスター化インデックスをチェックしない (NOINDEX)] を選択します。

SQL Serverデータベースは、Microsoft SQL ServerのDatabase Consistency Checker (DBCC) を使用して、データベース内のオブジェクトの論理的な整合性と物理的な整合性をチェックします。

- v. 内部データベース スナップショットを使用する代わりにチェックを制限し、ロックを取得するには、[内部データベース スナップショット コピーを使用する代わりにチェックを制限し、ロックを取得する (**TABLOCK**)] を選択します。

- c. ログ バックアップ セクションで、完了時にログ バックアップを検証する を選択して、完了時にログ バックアップを検証します。

- d. *検証スクリプト設定*セクションで、検証操作の前または後に実行するプレスクリプトまたはポストスクリプトのパスと引数を入力します。

- 8. 概要を確認し、[完了] をクリックします。

リソース グループの作成とSQLバックアップ ポリシーの適用

リソース グループはコンテナであり、バックアップして保護するリソースをここに追加する必要があります。

リソース グループを使用することで、特定のアプリケーションに関連するすべてのデータを同時にバックアップできます。リソース グループはいずれのデータ保護ジョブにも必要になります。リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義することも必要です。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name] ページで、次の操作を実行します。

フィールド	操作
Name	リソース グループの名前を入力します。
Tags	リソース グループを検索しやすくするために、ラベルを入力します。

フィールド	操作
Use custom name format for Snapshot copy	Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。

4. [リソース] ページで、[ホスト] ドロップダウン リストからホスト名を選択し、[リソース タイプ] ドロップダウン リストからリソース タイプを選択します。
5. *利用可能なリソース*セクションからリソースを選択し、右矢印をクリックして*選択したリソース*セクションに移動します。
6. [Policies] ページで、次の手順を実行します。
 - a. ドロップダウン リストから1つ以上のポリシーを選択します。
 - b. スケジュールの設定列で*をクリックします。  * 設定するポリシーの。
 - c. ポリシー *policy_name* のスケジュールの追加ダイアログ ボックスでスケジュールを構成し、[OK] をクリックします。
 - d. [Microsoft SQL Server scheduler]を選択します。
7. [Verification] ページで、次の手順を実行します。
 - a. 検証サーバを選択します。
 - b. 検証スケジュールを設定するポリシーを選択し、*をクリックします。  *。
 - c. *バックアップ後に検証を実行*または*スケジュールされた検証を実行*を選択します。
 - d. [OK]をクリックします。
8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。
9. 概要を確認し、[完了] をクリックします。

Azure NetApp Filesで実行されているSQL Serverデータベースのバックアップ

どのリソース グループにもまだ含まれていないリソースは、[Resources] ページからバックアップすることができます。

開始する前に

Azure Windows フェイルオーバー クラスタにクラスタIPが割り当てられていない場合や、SnapCenterから到達できない場合は、ロード バランサを作成する必要があります。ロード バランサのIPが設定され、SnapCenter Serverから到達可能である必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストから データベース、インスタンス、または 可用性グループ を選択します。
3. [リソース] ページで、[スナップショット コピーにカスタム名形式を使用する] を選択し、スナップショット名に使用するカスタム名形式を入力します。

4. [Policies]ページで、次の手順を実行します。
 - a. ドロップダウン リストから1つ以上のポリシーを選択します。
 - b. を選択  スケジュールを構成するポリシーの [スケジュールの構成] 列で、
 - c. ポリシー *policy_name* のスケジュールの追加 ダイアログ ボックスでスケジュールを構成し、[OK] を選択します。

policy_name は選択したポリシーの名前です。
 - d. **Microsoft SQL Server** スケジューラを使用する*を選択し、スケジュール ポリシーに関連付けられている *スケジューラ インスタンス ドロップダウン リストからスケジューラ インスタンスを選択します。
5. [Verification]ページで、次の手順を実行します。
 - a. 検証サーバを選択します。
 - b. 検証スケジュールを設定するポリシーを選択し、*をクリックします。  *。
 - c. *バックアップ後に検証を実行*または*スケジュールされた検証を実行*を選択します。
 - d. [OK]をクリックします。
6. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。
7. 概要を確認し、[完了] をクリックします。
8. *今すぐバックアップ*を選択します。
9. [Backup]ページで次の手順を実行します。
 - a. リソースに複数のポリシーが関連付けられている場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。
 - b. *バックアップ後に検証*を選択します。
 - c. *バックアップ*を選択します。
10. モニター > ジョブ をクリックして、操作の進行状況を監視します。

SQL Serverリソース グループのバックアップ

複数のリソースで構成されるリソース グループをバックアップできます。リソース グループのバックアップ処理は、リソース グループに定義されているすべてのリソースを対象に実行されます。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。
3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] を選択します。
4. [Backup]ページで次の手順を実行します。

- a. リソース グループに複数のポリシーが関連付けられている場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。
 - b. バックアップ後、「検証」を選択してオンデマンド バックアップを検証します。
 - c. *バックアップ*を選択します。
5. モニター > ジョブ を選択して、操作の進行状況を監視します。

SQL Serverデータベースのリストアとリカバリ

SnapCenterを使用して、バックアップされたSQL Serverデータベースをリストアすることができます。データベース リストアは段階的に実施され、すべてのデータとログ ページが指定したSQL Serverバックアップから指定したデータベースにコピーされます。

タスク概要

リストアのターゲット インスタンスに、SMB ADActiveディレクトリ ドメインに属し、ファイル権限を適切に設定する権限があるActive Directoryユーザが設定されていることを確認する必要があります。クレデンシャルは、SnapCenterでインスタンス レベルで設定する必要があります。

ターゲット インスタンスのSQL認証は、SMB構成ではサポートされません。ターゲット インスタンスは、必要な権限を持つActive Directoryユーザを使用してSnapCenterで設定する必要があります。

SnapCenter Plug-inサービスのサービス アカウントがActive Directoryユーザでない場合は、別のホストへのリストアの実行中にこれを偽装して必要な処理を実行できるように、ソース ボリュームを完全に制御できるユーザが必要です。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから データベース または リソース グループ を選択します。
3. リストからデータベースまたはリソース グループを選択します。
4. [コピーの管理] ビューで、ストレージ システムから [バックアップ] を選択します。
5. 表からバックアップを選択し、 アイコン。
6. [Restore Scope] ページで、次のいずれかのオプションを選択します。
 - a. バックアップが作成されたのと同じ SQL サーバーにデータベースを復元する場合は、「バックアップが作成されたのと同じホストにデータベースを復元する」を選択します。
 - b. バックアップが作成されたのと同じホストまたは別のホスト内の別の SQL サーバーにデータベースを復元する場合は、「データベースを別のホストに復元」を選択します。
7. [Recovery Scope] ページで、次のいずれかのオプションを選択します。
 - a. ログなしで完全バックアップのみを復元する必要がある場合は、「なし」を選択します。
 - b. 完全バックアップ後に利用可能なすべてのログ バックアップを復元するには、すべてのログ バックアップ 最新バックアップ復元操作を選択します。
 - c. ログ バックアップ別 を選択すると、ポイントインタイム復元操作が実行され、選択した日付のバックアップ ログまでのバックアップ ログに基づいてデータベースが復元されます。
 - d. 復元されたデータベースにトランザクション ログが適用されなくなる日時を指定するには、[特定の日

付まで] を選択します。

- e. すべてのログ バックアップ、ログ バックアップ別、または*特定の日付まで*を選択し、ログがカスタムの場所に配置されている場合は、*カスタム ログ ディレクトリを使用する*を選択し、ログの場所を指定します。
8. [Pre-Ops and Post Ops]ページで、必要な詳細を指定します。
9. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。
10. 概要を確認し、[完了] をクリックします。
11. モニター > ジョブ ページを使用して復元プロセスを監視します。

SQL Serverデータベースのバックアップのクローニング

SnapCenter を使用すると、データベースのバックアップを使用して SQL データベースのクローンを作成できます。作成されるクローンはシック クローンであり、親容量プール上に作成されます。

タスク概要

クローニングのターゲット インスタンスに、SMB ADActiveディレクトリ ドメインに属し、ファイル権限を適切に設定する権限があるActive Directoryユーザが設定されていることを確認する必要があります。クレデンシャルは、SnapCenterでインスタンス レベルで設定する必要があります。

ターゲット インスタンスのSQL認証は、SMB構成ではサポートされません。ターゲット インスタンスは、必要な権限を持つActive Directoryユーザを使用してSnapCenterで設定する必要があります。

SnapCenter Plug-inサービスのサービス アカウントがActive Directoryユーザでない場合は、クローニングの実行中にこれを偽装して必要な処理を実行できるように、ソース ボリュームを完全に制御できるユーザが必要です。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] または [リソース グループ] を選択します。
3. データベースまたはリソース グループを選択します。
4. コピーの管理 ビュー ページで、プライマリ ストレージ システムからのバックアップを選択します。
5. バックアップを選択し、*を選択します。  *。
6. クローン オプション ページで、必要な詳細をすべて入力します。
7. [Location]ページで、クローンを作成するストレージの場所を選択します。

SQL ServerデータベースANFボリュームが手動QoS容量プールに設定されている場合は、クローン ボリュームのQoSを指定します。

クローン ボリュームにQoSが指定されていない場合は、ソース ボリュームのQoSが使用されます。自動QoS容量プールを使用している場合、指定したQoS値は無視されます。

8. [Logs]ページで、次のいずれかのオプションを選択します。

- a. ログなしで完全なバックアップのみをクローンする場合は、「なし」を選択します。
 - b. 完全バックアップ以降の日付の利用可能なすべてのログ バックアップを複製する場合は、[すべてのログ バックアップ]を選択します。
 - c. 選択した日付のバックアップ ログまでに作成されたバックアップ ログに基づいてデータベースのクローンを作成する場合は、[次のログ バックアップまで]を選択します。
 - d. 指定した日時以降にトランザクション ログを適用しない場合は、[特定の日付まで]を選択します。
9. スクリプト ページで、スクリプトのタイムアウト、パス、およびクローン操作の前または後に実行するプレスクリプトまたはポストスクリプトの引数をそれぞれ入力します。
 10. *通知*ページの*電子メール設定*ドロップダウンリストから、電子メールを送信するシナリオを選択します。
 11. 概要を確認し、[完了]を選択します。
 12. モニター > ジョブ を選択して、操作の進行状況を監視します。

クローン ライフサイクルの実行

SnapCenterを使用して、リソース グループまたはデータベースからクローンを作成できます。クローニングはオンデマンドで実行することも、リソース グループまたはデータベースに対して定期的なクローニング処理をスケジュール設定することもできます。バックアップを定期的にクローニングすると、クローンを使用してアプリケーションの開発、データの取り込み、またはデータのリカバリを行うことができます。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [データベース] または [リソース グループ] を選択します。
3. データベースまたはリソース グループを選択します。
4. コピーの管理 ビュー ページで、プライマリ ストレージ システムからのバックアップを選択します。
5. バックアップを選択し、*を選択します。  *。
6. クローン オプション ページで、必要な詳細をすべて入力します。
7. [Location] ページで、クローンを作成するストレージの場所を選択します。

SQL ServerデータベースANFボリュームが手動QoS容量プールに設定されている場合は、クローン ボリュームのQoSを指定します。

クローン ボリュームにQoSが指定されていない場合は、ソース ボリュームのQoSが使用されます。自動QoS容量プールを使用している場合、指定したQoS値は無視されます。

8. スクリプト ページで、スクリプトのタイムアウト、パス、およびクローン操作の前または後に実行するプレスクリプトまたはポストスクリプトの引数をそれぞれ入力します。
9. [Schedule] ページで、次のいずれかを実行します。
 - クローンジョブをすぐに実行するには、[今すぐ実行] を選択します。
 - クローン操作を実行する頻度、クローン スケジュールを開始する日時、クローン操作を実行する日、スケジュールの有効期限、スケジュールの有効期限が切れた後にクローンを削除するかどうかを決定する場合は、[スケジュールの構成] を選択します。
10. *通知*ページの*電子メール設定*ドロップダウンリストから、電子メールを送信するシナリオを選択しま

す。

11. 概要を確認し、[完了] を選択します。
12. モニター > ジョブ を選択して、操作の進行状況を監視します。

Oracleデータベースの保護

ホストの追加とSnapCenter Plug-in for Oracle Databaseのインストール

[Add Host]ページを使用してホストを追加し、SnapCenter Plug-ins Package for LinuxまたはSnapCenter Plug-ins Package for AIXをインストールできます。プラグインは、自動的にリモート ホストにインストールされます。

ホストの追加とプラグイン パッケージのインストールは、ホストごとまたはクラスタごとに実行できます。クラスタ（Oracle RAC）にプラグインをインストールする場合、プラグインはクラスタのすべてのノードにインストールされます。Oracle RAC One Nodeの場合は、このプラグインをアクティブ ノードとパッシブ ノードの両方にインストールする必要があります。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. *管理対象ホスト*タブが選択されていることを確認します。
3. *[追加]*をクリックします。
4. [Hosts]ページで、次の操作を実行します。
 - a. [Host Type]フィールドで、ホスト タイプを選択します。
 - b. [Host name]フィールドに、ホストの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。
 - c. [Credentials]フィールドに、作成したクレデンシャルを入力します。
5. [Select Plug-ins to Install]セクションで、インストールするプラグインを選択します。
6. (オプション) [その他のオプション] をクリックして詳細を指定します。
7. *送信*をクリックします。
8. 指紋を確認して、「確認して送信」をクリックします。

クラスタ セットアップでは、クラスタ内の各ノードのフィンガープリントを検証する必要があります。

9. インストールの進捗状況を監視します。

Oracleデータベースのバックアップ ポリシーの作成

SnapCenterを使用してOracleデータベース リソースをバックアップする前に、バックアップ対象のリソースまたはリソース グループのバックアップ ポリシーを作成する必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。

2. [設定]ページで、[ポリシー]をクリックします。
3. ドロップダウン リストから[Oracle Database]を選択します。
4. *新規*をクリックします。
5. [Name]ページで、ポリシーの名前と説明を入力します。
6. ポリシー タイプ ページで、次の手順を実行します。
 - a. ストレージの種類として * Azure NetApp Files* を選択します。
 - b. バックアップ タイプとして、オンライン バックアップまたはオフライン バックアップを選択します。
 - c. Oracle Recovery Manager (RMAN) を使用してバックアップをカタログ化する場合は、「**Oracle Recovery Manager (RMAN)** を使用したバックアップのカタログ化」を選択します。
 - d. バックアップ後にアーカイブ ログを削除する場合は、[バックアップ後にアーカイブ ログを削除する]を選択します。
 - e. アーカイブ ログの削除設定を指定します。
7. スナップショットとバックアップ ページで、次の手順を実行します。
 - a. スケジュールされたバックアップの頻度を選択します。
 - b. 保持設定を指定します。
 - c. Azure NetApp Filesバックアップを有効にする場合は、[バックアップを有効にする]を選択し、保持設定を指定します。
8. [Script]ページで、バックアップ処理の前またはあとに実行するプリスクリプトまたはポストスクリプトのパスと引数を入力します。
9. [Verification]ページで、検証処理を実行するバックアップ スケジュールを選択し、検証処理の前後に実行するプリスクリプトまたはポストスクリプトのパスと引数をそれぞれ入力します。
10. 概要を確認し、[完了] をクリックします。

リソース グループの作成とOracleバックアップ ポリシーの適用

リソース グループはコンテナであり、バックアップして保護するリソースをここに追加する必要があります。

リソース グループを使用することで、特定のアプリケーションに関連するすべてのデータを同時にバックアップできます。リソース グループはいずれのデータ保護ジョブにも必要になります。リソース グループに1つ以上のポリシーを適用して、実行するデータ保護ジョブのタイプを定義することも必要です。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[新しいリソース グループ] をクリックします。
3. [Name]ページで、次の操作を実行します。

フィールド	操作
Name	リソース グループの名前を入力します。

フィールド	操作
Tags	リソース グループを検索しやすくするために、ラベルを入力します。
Use custom name format for Snapshot copy	Snapshot名にカスタムの名前形式を使用する場合は、このチェック ボックスをオンにして名前形式を入力します。
Archive log file destination	アーカイブ ログ ファイルのデスティネーションを指定します。

4. [リソース] ページで、[ホスト] ドロップダウン リストからホスト名を選択し、[リソース タイプ] ドロップダウン リストからリソース タイプを選択します。
5. *利用可能なリソース*セクションからリソースを選択し、右矢印をクリックして*選択したリソース*セクションに移動します。
6. [Policies] ページで、次の手順を実行します。
 - a. ドロップダウン リストから1つ以上のポリシーを選択します。
 - b. スケジュールの設定列で*をクリックします。  * 設定するポリシーの。
 - c. ポリシー *policy_name* のスケジュールの追加ダイアログ ボックスでスケジュールを構成し、[OK] をクリックします。
7. [Verification] ページで、次の手順を実行します。
 - a. 検証サーバを選択します。
 - b. 検証スケジュールを設定するポリシーを選択し、*をクリックします。  。
 - c. *バックアップ後に検証を実行*または*スケジュールされた検証を実行*を選択します。
 - d. [OK] をクリックします。
8. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。
9. 概要を確認し、[完了] をクリックします。

Azure NetApp Filesで実行されているOracleデータベースのバックアップ

どのリソース グループにもまだ含まれていないリソースは、[Resources] ページからバックアップすることができます。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. リソース ページで、表示ドロップダウン リストから データベース を選択します。
3. [リソース] ページで、[スナップショット コピーにカスタム名前形式を使用する] を選択し、スナップショット名に使用するカスタム名前形式を入力します。

4. [Policies]ページで、次の手順を実行します。
 - a. ドロップダウン リストから1つ以上のポリシーを選択します。
 - b.  を選択  スケジュールを構成するポリシーの [スケジュールの構成] 列で、
 - c. ポリシー *policy_name* のスケジュールの追加 ダイアログ ボックスでスケジュールを構成し、[OK] を選択します。
5. [Verification]ページで、次の手順を実行します。
 - a. 検証サーバを選択します。
 - b.  検証スケジュールを設定するポリシーを選択し、*をクリックします。  *。
 - c. *バックアップ後に検証を実行*または*スケジュールされた検証を実行*を選択します。
 - d. [OK]をクリックします。
6. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。
7. 概要を確認し、[完了] をクリックします。
8. *今すぐバックアップ*を選択します。
9. [Backup]ページで次の手順を実行します。
 - a. リソースに複数のポリシーが関連付けられている場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。
 - b. *バックアップ*をクリックします。
10. モニター > ジョブ をクリックして、操作の進行状況を監視します。

Oracleリソース グループのバックアップ

複数のリソースで構成されるリソース グループをバックアップできます。リソース グループのバックアップ処理は、リソース グループに定義されているすべてのリソースを対象に実行されます。

手順

1. 左側のナビゲーション ペインで [リソース] を選択し、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。
3. [リソース グループ] ページで、バックアップするリソース グループを選択し、[今すぐバックアップ] を選択します。
4. [Backup]ページで次の手順を実行します。
 - a. リソース グループに複数のポリシーが関連付けられている場合は、[ポリシー] ドロップダウン リストから、バックアップに使用するポリシーを選択します。
 - b. *バックアップ*を選択します。
5. モニター > ジョブ を選択して、操作の進行状況を監視します。

Oracleデータベースのリストアとリカバリ

データ損失が発生した場合は、SnapCenterを使用して1つ以上のバックアップからアクティブ ファイルシステムにデータをリストアし、そのあとにデータベースをリカバリできます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから データベース または リソース グループ を選択します。
3. リストからデータベースまたはリソース グループを選択します。
4. [コピーの管理] ビューで、プライマリ ストレージ システムから [バックアップ] を選択します。
5. 表からバックアップを選択し、*をクリックします。*。
6. [Restore Scope] ページで、次の作業を実行します。
 - a. RAC環境でデータベースのバックアップを選択した場合は、[RAC]を選択します。
 - b. 次の操作を実行します。
 - i. データベース ファイルのみを復元する場合は、[すべてのデータファイル] を選択します。
 - ii. 表領域のみを復元する場合は、「表領域」を選択します。
 - iii. Data Guard スタンバイ データベースまたは Active Data Guard スタンバイ データベースの REDO ログ ファイルを復元する場合は、**REDO** ログ ファイル を選択します。
 - iv. プラガブル データベース を選択し、復元する PDB を指定します。
 - v. プラガブル データベース (**PDB**) 表領域 を選択し、復元する PDB とその PDB の表領域を指定します。
 - vi. バックアップが作成されたのと同じ SQL サーバーにデータベースを復元する場合は、「バックアップが作成されたのと同じホストにデータベースを復元する」を選択します。
 - vii. バックアップが作成されたのと同じホストまたは別のホスト内の別の SQL サーバーにデータベースを復元する場合は、「データベースを別のホストに復元」を選択します。
 - viii. データベースの状態を復元および回復操作を実行するために必要な状態に変更するには、「復元および回復に必要な場合はデータベースの状態を変更する」を選択します。
 - ix. バックアップ後に新しいデータファイルが追加された場合や、LVM ディスク グループに LUN が追加、削除、または再作成された場合にインプレース リストアを実行する場合は、[強制インプレース リストア] を選択します。
7. [Recovery Scope] ページで、次のいずれかのオプションを選択します。
 - a. 最後のトランザクションまで回復する場合は、「すべてのログ」を選択します。
 - b. 特定の SCN まで回復する場合は、**SCN** (システム変更番号) まで を選択します。
 - c. 特定の日付と時刻に復元する場合は、「日付と時刻」を選択します。
 - d. 回復したくない場合は、「回復なし」を選択します。
 - e. 外部アーカイブ ログ ファイルの場所を指定する場合は、[外部アーカイブ ログの場所を指定する] を選択します。

8. [Pre-Ops and Post Ops]ページで、必要な詳細を指定します。
9. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。
10. 概要を確認し、[完了] をクリックします。
11. モニター > ジョブ をクリックして、操作の進行状況を監視します。

ポイントインタイム リカバリを使用した表領域のリストアとリカバリ

破損または削除された表領域のサブセットは、データベース内の他の表領域に影響を与えることなくリストアできます。SnapCenterは、RMANを使用して表領域のポイントインタイムリカバリ（PITR）を実行します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから データベース または リソース グループ を選択します。
3. タイプが単一インスタンス（マルチテナント）のデータベースを選択します。
4. [コピーの管理] ビューで、ストレージ システムから [バックアップ] を選択します。

バックアップがカタログ化されていない場合は、バックアップを選択し、「カタログ」をクリックする必要があります。

5. カタログ化されたバックアップを選択し、*をクリックします。  *。
6. [Restore Scope]ページで、次の作業を実行します。
 - a. RAC 環境のデータベースのバックアップを選択した場合は、**RAC** を選択します。
 - b. 表領域のみを復元する場合は、「表領域」を選択します。
 - c. データベースの状態を復元および回復操作を実行するために必要な状態に変更するには、「復元および回復に必要な場合はデータベースの状態を変更する」を選択します。
7. [Recovery Scope]ページで、次のいずれかのオプションを選択します。
 - a. 特定の SCN まで回復する場合は、**SCN** (システム変更番号) まで を選択します。
 - b. 特定の日付と時刻に復元する場合は、「日付と時刻」を選択します。
8. [Pre-Ops and Post Ops]ページで、必要な詳細を指定します。
9. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。
10. 概要を確認し、[完了] をクリックします。
11. モニター > ジョブ ページを使用して復元プロセスを監視します。

ポイントインタイム リカバリを使用したプラガブル データベースのリストアとリカバリ

破損または削除されたプラガブル データベース（PDB）は、コンテナ データベース（CDB）内の他のPDBに影響を与えることなくリストアおよびリカバリできます。SnapCenterは、RMANを使用してPDBのポイントインタイム リカバリ（PITR）を実行します。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから データベース または リソース グループ を選択します。
3. タイプが単一インスタンス（マルチテナント）のデータベースを選択します。
4. [コピーの管理] ビューで、ストレージ システムから [バックアップ] を選択します。

バックアップがカタログ化されていない場合は、バックアップを選択し、「カタログ」をクリックする必要があります。

5. カタログ化されたバックアップを選択し、*をクリックします。*。
6. [Restore Scope] ページで、次の作業を実行します。
 - a. RAC 環境のデータベースのバックアップを選択した場合は、**RAC** を選択します。
 - b. PDBとPDB内の表領域のどちらをリストアするかに応じて、次のいずれかの操作を実行します。
 - PDB を復元する場合は、プラグブル データベース (**PDB**) を選択します。
 - PDB 内の表領域を復元する場合は、プラグブル データベース (**PDB**) 表領域 を選択します。
7. [Recovery Scope] ページで、次のいずれかのオプションを選択します。
 - a. 特定の SCN まで回復する場合は、**SCN** (システム変更番号) まで を選択します。
 - b. 特定の日付と時刻に復元する場合は、「日付と時刻」を選択します。
8. [Pre-Ops and Post Ops] ページで、必要な詳細を指定します。
9. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。
10. 概要を確認し、[完了] をクリックします。
11. モニター > ジョブ ページを使用して復元プロセスを監視します。

Oracleデータベースのバックアップのクローニング

SnapCenterを使用すると、データベースのバックアップ機能でOracleデータベースをクローニングできます。作成されるクローンはシック クローンであり、親容量プール上に作成されます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから データベース または リソース グループ を選択します。
3. データベースを選択します。
4. [Manage Copies]ビュー ページで、プライマリ ストレージ システムからバックアップを選択します。
5. データバックアップを選択し、*をクリックします。*。
6. [Name] ページで、データベース（CDBまたは非CDB）をクローニングするか、プラグブル データベース（PDB）をクローニングするかを選択します。
7. [Locations] ページで、必要な詳細を指定します。

OracleデータベースANFボリュームが手動QoS容量プールに設定されている場合は、クローン ボリュームのQoSを指定します。

クローン ボリュームにQoSが指定されていない場合は、ソース ボリュームのQoSが使用されます。自動QoS容量プールを使用している場合、指定したQoS値は無視されます。

8. [Credentials]ページで、次のいずれかを実行します。

- a. sysユーザのクレデンシャル名には、クローン データベースのsysユーザ パスワードの定義に使用するクレデンシャルを選択します。
- b. ASM インスタンス資格情報名では、クローン ホスト上の ASM インスタンスへの接続に OS 認証が有効になっている場合は、「なし」を選択します。

有効でない場合は、[sys]ユーザ、またはクローン ホストに適用される「sysasm」権限を持つユーザが設定されたOracle ASMクレデンシャルを選択します。

9. [Pre-Ops]ページでプリスクリプトのパスと引数を指定し、[Database parameter settings]セクションで、データベースの初期化に使用される事前入力されたデータベース パラメータの値を変更します。

10. 事後操作ページでは、クローンされたデータベースの回復を実行するために、*データベースの回復*と*キャンセルまで*がデフォルトで選択されています。

- a. **[キャンセルまで]** を選択した場合、SnapCenter は、クローン作成対象として選択されたデータ バックアップの後のアーカイブ ログの連続したシーケンスを持つ最新のログ バックアップをマウントしてリカバリを実行します。
- b. 日付と時刻 を選択すると、SnapCenter は指定された日付と時刻までデータベースを回復します。
- c. **SCN** まで を選択すると、SnapCenter は指定された SCN までデータベースを回復します。
- d. 外部アーカイブ ログの場所を指定する を選択した場合、SnapCenter は指定された SCN または選択された日時に基づいて最適な数のログ バックアップを識別してマウントします。
- e. デフォルトでは、新しい **DBID** の作成 チェックボックスが選択されており、クローンされたデータベースとソース データベースを区別する一意の番号 (DBID) が生成されます。

ソース データベースのDBIDをクローン データベースに割り当てる場合は、このチェック ボックスをオフにします。このシナリオでは、ソース データベースがすでに登録されている外部のRMANカタログにクローン データベースを登録すると、処理は失敗します。

- f. クローンされたデータベースのデフォルトの一時表領域に一時ファイルを作成する場合は、「一時表領域用の一時ファイルを作成する」チェックボックスをオンにします。
- g. クローンの作成時に適用する **SQL** エントリを入力 で、クローンの作成時に適用する SQL エントリを追加します。
- h. *クローン操作後に実行するスクリプトを入力*で、クローン操作後に実行するポストスクリプトのパスと引数を指定します。

11. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。

12. 概要を確認し、[完了] を選択します。

13. モニター > ジョブ を選択して、操作の進行状況を監視します。

プラグブル データベースのクローニング

プラグブル データベース (PDB) は、同じホストまたは代替ホスト上の別のターゲットCDBまたは同じターゲットCDBにクローニングできます。クローニングされたPDBを目的のSCNまたは日時にリカバリすることもできます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから データベース または リソース グループ を選択します。
3. タイプが単一インスタンス (マルチテナント) のデータベースを選択します。
4. [Manage Copies]ビュー ページで、プライマリ ストレージ システムからバックアップを選択します。
5. バックアップを選択し、*をクリックします。  *。
6. 「名前」 ページで、「**PDB クローン**」を選択し、その他の詳細を指定します。
7. [Locations]ページで、必要な詳細を指定します。
8. [Pre-Ops]ページでプリスクリプトのパスと引数を指定し、[Database parameter settings]セクションで、データベースの初期化に使用される事前入力されたデータベース パラメータの値を変更します。
9. 事後操作ページでは、クローンされたデータベースのリカバリを実行するために、デフォルトで キャンセルまで が選択されます。
 - a. **[キャンセルまで]** を選択した場合、SnapCenter は、クローン作成対象として選択されたデータ バックアップの後のアーカイブ ログの連続したシーケンスを持つ最新のログ バックアップをマウントしてリカバリを実行します。
 - b. 日付と時刻 を選択すると、SnapCenter は指定された日付と時刻までデータベースを回復します。
 - c. 外部アーカイブ ログの場所を指定する を選択した場合、SnapCenter は指定された SCN または選択された日時に基づいて最適な数のログ バックアップを識別してマウントします。
 - d. デフォルトでは、新しい **DBID** の作成 チェックボックスが選択されており、クローンされたデータベースとソース データベースを区別する一意の番号 (DBID) が生成されます。

ソース データベースのDBIDをクローン データベースに割り当てる場合は、このチェック ボックスをオフにします。このシナリオでは、ソース データベースがすでに登録されている外部のRMANカタログにクローン データベースを登録すると、処理は失敗します。
 - e. クローンされたデータベースのデフォルトの一時表領域に一時ファイルを作成する場合は、「一時表領域用の一時ファイルを作成する」チェックボックスをオンにします。
 - f. クローンの作成時に適用する **SQL** エントリを入力 で、クローンの作成時に適用する SQL エントリを追加します。
 - g. *クローン操作後に実行するスクリプトを入力*で、クローン操作後に実行するポストスクリプトのパスと引数を指定します。
10. 通知ページの 電子メール設定 ドロップダウン リストから、電子メールを送信するシナリオを選択します。
11. 概要を確認し、[完了] を選択します。
12. モニター > ジョブ を選択して、操作の進行状況を監視します。

SnapCenter Serverとプラグインの管理

ダッシュボードの表示

ダッシュボードの概要

SnapCenterの左側のナビゲーション ペインから、ダッシュボードを使用してシステムの健全性を確認できます。ダッシュボードには、最近のジョブ アクティビティ、アラート、保護の概要、ストレージの効率化と使用状況、SnapCenterのジョブ（バックアップ、クローニング、リストア）のステータス、スタンドアロン / Windows クラスタ ホストの構成ステータス、SnapCenterで管理しているStorage Virtual Machine（SVM）の数、ライセンス容量などの情報が表示されます。

ダッシュボード ビューに表示される情報は、SnapCenterに現在ログインしているユーザに割り当てられたロールによって異なります。ユーザに表示権限がない情報は表示されないことがあります。

多くの場合、**i**にマウスを合わせると、ディスプレイに関する詳細情報を表示できます。場合によっては、ダッシュボードに表示される情報は、リソース、モニター、レポートなどのSnapCenter GUI ページの詳細なソース情報にリンクされます。

最近のジョブ アクティビティ

[Recent Job Activities] タイルには、アクセス可能なバックアップ、リストア、およびクローニング ジョブの最新のジョブ アクティビティが表示されます。この表示内のジョブの状態は、完了、警告、失敗、実行中、キューに登録済み、キャンセル済みのいずれかです。

ジョブにカーソルを合わせると、詳細が表示されます。ジョブ番号をクリックすると[Monitor]ページにリダイレクトされ、その他のジョブ情報を確認できます。そこからジョブの詳細またはログ情報を取得し、そのジョブに固有のレポートを生成できます。

すべてのSnapCenterジョブの履歴を表示するには、[すべて表示] をクリックします。

アラート

[Alerts] タイルには、ホストおよびSnapCenter Serverに関する未解決の重大アラートと警告アラートについての最新情報が表示されます。

重大アラートと警告アラートの総数がタイル上部に表示されます。重大または警告の合計をクリックすると[Alerts]ページにリダイレクトされ、[Alerts]ページに対応するフィルタが適用されます。

特定のアラートをクリックすると、そのアラートの詳細が表示された[Alerts]ページにリダイレクトされます。画面下部の「すべて表示」をクリックすると、「アラート」ページにリダイレクトされ、すべてのアラートのリストが表示されます。

最新の保護サマリ

[Latest Protection Summary] タイルには、アクセス可能なすべてのエンティティの保護ステータスが表示されます。デフォルトでは、すべてのプラグインのステータスが表示されます。Snapshotとしてプライマリ ストレージにバックアップされたリソース、およびSnapMirrorテクノロジーとSnapVaultテクノロジーを使用してセカ

ンダリ ストレージにバックアップされたリソースのステータス情報が提供されます。セカンダリ ストレージの保護ステータス情報が表示されるかどうかは、選択したプラグインのタイプに基づきます。



mirror-vault保護ポリシーを使用している場合、保護サマリのカウンタはSnapMirrorではなくSnapVaultの概要チャートに表示されます。

ドロップダウン メニューからプラグインを選択すると、個々のプラグインの保護ステータスを確認できます。ドーナツグラフは、選択したプラグインの保護対象リソースの割合を示します。ドーナツグラフのスライスをクリックすると、「レポート > プラグイン」ページにリダイレクトされ、指定したプラグインのすべてのプライマリストレージおよびセカンダリストレージアクティビティの詳細なレポートが表示されます。



セカンダリ ストレージに関するレポートはSnapVaultのみに適用されます。SnapMirrorレポートはサポートされません。



SAP HANAの場合、Snapshotについては、プライマリ ストレージとセカンダリ ストレージの保護ステータス情報が提供されます。ファイルベースのバックアップについては、プライマリストレージの保護ステータスのみが提供されます。

保護ステータス	プライマリ ストレージ	セカンダリ ストレージ
失敗	バックアップに失敗したリソースグループに属しているエンティティの数	セカンダリ デスティネーションへのバックアップの転送に失敗したエンティティの数
成功	バックアップに成功したリソースグループに属しているエンティティの数	セカンダリ デスティネーションへのバックアップの転送に成功したエンティティの数
未設定	どのリソース グループにも属しておらず、バックアップされていないエンティティの数	バックアップをセカンダリ デスティネーションに転送するように設定されていないリソース グループに属しているエンティティの数
未開始	リソース グループに属しているが、バックアップが実行されていないエンティティの数	該当なし。



SnapCenter Server 4.2 と以前のバージョンのプラグイン (4.2 より前) を使用してバックアップを作成している場合、「最新の保護の概要」タイルにこれらのバックアップのSnapMirror保護ステータスは表示されません。

ジョブ

[Jobs]タイルには、アクセス可能なバックアップ、リストア、およびクローニング ジョブの概要が表示されます。ドロップダウン メニューを使用して、レポートの期間をカスタマイズできます。オプションは、過去24時間、過去7日間、および過去30日間です。デフォルトでは、過去7日間に実行されたデータ保護ジョブの情報がレポートされます。

バックアップ、リストア、およびクローニング ジョブの情報がドーナツ チャートに表示されます。ドーナツ

チャートのスライスをクリックすると、選択したジョブにフィルタされた[Monitor]ページにリダイレクトされます。

ジョブ ステータス	説明
失敗	失敗したジョブ数。
警告	エラーが発生したジョブ数。
成功	成功したジョブ数。
実行中	実行中のジョブ数。

ストレージ

[Storage]タイルには、過去90日間に保護ジョブで使用されたプライマリ ストレージとセカンダリ ストレージ容量が表示されます。傾向を表すグラフとプライマリ ストレージの削減量も表示されます。ストレージ情報は毎日深夜0時に更新されます。

その日の使用容量の合計として、SnapCenterで使用可能なバックアップの総数とそれらのバックアップが占有するサイズがタイル上部に表示されます。1つのバックアップに複数のSnapshotが関連付けられている場合、それらも同じようにカウントされます。これは、プライマリとセカンダリの両方のSnapshotに当てはまります。たとえばバックアップを10個作成し、そのうちの2個はポリシーに基づいて削除され、1個はユーザーが削除したとします。この場合、バックアップ数は7個と表示され、それらの7個のバックアップが占有するサイズが表示されます。

プライマリ ストレージのストレージ削減率は、プライマリ ストレージの物理容量に対する論理容量（クローンおよびSnapshotによる削減量とストレージ使用量の合計）の比率です。棒グラフはストレージ削減量を表しています。

線グラフには、過去90日間について、プライマリとセカンダリそれぞれの1日のストレージ使用量が表示されます。グラフにカーソルを合わせると、その日の詳細なデータが表示されます。



SnapCenter Server 4.2 と以前のバージョンのプラグイン (4.2 より前) を使用してバックアップを作成する場合、[ストレージ] タイルに、バックアップの数、これらのバックアップによって消費されるストレージ、スナップショットの節約、クローンの節約、およびスナップショットのサイズが表示されません。

構成

[Configuration]タイルには、SnapCenterで管理しているスタンドアロンとWindowsクラスタのホストについて、アクセス可能なすべてのアクティブなホストのステータス情報がまとめて表示されます。これには、ホストに関連付けられているプラグインのステータス情報も含まれます。

[Hosts]の横にある数字をクリックすると、[ホスト]ページの[管理対象ホスト]セクションにリダイレクトされます。そのページから、選択したホストの詳細情報を取得できます。

さらにこのタイルには、SnapCenterで管理しているアクセス可能なスタンドアロンのONTAP SVMとクラスタのONTAP SVMの合計数が表示されます。[SVM]の横にある数字をクリックすると、[Storage Systems]ページにリダイレクトされます。そのページから、選択したSVMの詳細情報を取得できます。

ホストの設定状態は赤（重大）、黄（警告）、緑（アクティブ）で、それぞれの状態のホストの数が表示されます。ステータス メッセージも表示されます。

設定ステータス	説明
アップグレードが必要	サポートされていないプラグインを実行していてアップグレードが必要なホストの数。サポートされていないプラグインは、このバージョンのSnapCenterでは使用できません。
移行が必要	サポートされていないプラグインを実行していて移行が必要なホストの数。サポートされていないプラグインは、このバージョンのSnapCenterでは使用できません。
インストール済みプラグインなし	正常に追加されたがプラグインのインストールが必要であるホスト、またはプラグインのインストールに失敗したホストの数。
中断	スケジュールが中断されてメンテナンス中のホストの数。
停止	稼働しているがプラグイン サービスが実行されていないホストの数。
ホスト停止	停止しているか到達できないホストの数。
アップグレード可能（オプション）	新しいバージョンのプラグイン パッケージにアップグレード可能なホストの数。
移行可能（オプション）	新しいバージョンのプラグインに移行可能なホストの数。
ログ ディレクトリを設定	SCSQLでトランザクション ログ バックアップを作成するためにログ ディレクトリの設定が必要なホストの数。
VMware プラグインを設定	SnapCenter Plug-in for VMware vSphereの追加が必要なホストの数。
不明	登録は完了しているがインストールが開始されていないホストの数。
実行中	稼働していてプラグインが実行されているホストの数。SCSQLプラグインの場合は、ログ ディレクトリとハイパーバイザーも設定されている。

設定ステータス	説明
プラグインをインストール中 / アンインストール中	プラグインのインストールまたはアンインストールを実行中のホストの数。

ダッシュボードに情報を表示する方法

SnapCenterの左側のナビゲーション ペインから、さまざまなダッシュボードのタイル（表示領域）と関連するシステムの詳細を表示できます。ダッシュボードに表示できるタイル数は決まっていて、変更することはできません。各タイルに表示される内容は、ロールベース アクセス制御（RBAC）に基づいて決まります。

手順

1. 左側のナビゲーション ペインで、[ダッシュボード] をクリックします。
2. 各タイルのアクティブな領域をクリックすると、追加情報が表示されます。

たとえば、「ジョブ」のドーナツ グラフをクリックすると、選択内容の詳細情報を表示する「モニター」ページにリダイレクトされます。保護の概要 のドーナツ グラフをクリックすると、レポート ページにリダイレクトされ、選択内容に関する詳細情報が表示されます。

ダッシュボードからのジョブ ステータス レポートのリクエスト

[Dashboard]ページからバックアップ、リストア、およびクローニング ジョブに関するレポートを表示できます。SnapCenter環境で成功または失敗したジョブの総数を確認する場合に便利です。

手順

1. 左側のナビゲーションペインで*ダッシュボード*をクリックします。
2. ダッシュボードでジョブ タイルを見つけて、バックアップ、復元、または*クローン*を選択します。
3. プルダウン メニューを使用して、ジョブ情報を表示する期間 (24 時間、7 日間、または 30 日間) を選択します。

ドーナツ チャートにデータが表示されます。

4. レポートを表示するジョブ情報に対応するドーナツ チャートのスライスをクリックします。

ドーナツ チャートをクリックすると、[Dashboard]ページから[Monitor]ページにリダイレクトされます。[モニター]ページには、ドーナツ チャートで選択したステータスのジョブが表示されます。

5. [Monitor]ページのリストで、特定のジョブをクリックして選択します。
6. モニター ページの上部にある [レポート] をクリックします。

結果

レポートには、選択したジョブの情報のみが表示されます。レポートは画面で確認するか、またはローカル

システムにダウンロードできます。

ダッシュボードからの保護ステータス レポートのリクエスト

ダッシュボードを使用して、特定のプラグインで管理されるリソースの保護の詳細を表示できます。データ保護サマリには、データ バックアップの情報のみが表示されます。

手順

1. 左側のナビゲーション ペインで、[ダッシュボード] をクリックします。
2. ダッシュボードで[Latest Protection Summary]タイルで、プルダウン メニューを使用してプラグインを選択します。

ダッシュボードには、プライマリ ストレージにバックアップされたリソースのドーナツ チャートが表示され、プラグインによってはセカンダリ ストレージにバックアップされたリソースのドーナツ チャートも表示されます。



データ保護レポートを使用できるのは、特定のタイプのプラグインのみです。*すべてのプラグイン*の指定はサポートされていません。

3. レポートを表示するステータスに対応するドーナツ チャートのスライスをクリックします。

ドーナツ チャートをクリックすると、[Dashboard]ページから[Reports]ページへ、さらに[Plug-in]ページへリダイレクトされます。レポートには、選択したプラグインのステータスのみが表示されます。レポートは画面で確認するか、またはローカル システムにダウンロードできます。



SnapMirrorのドーナツ チャートおよびファイルベースのSAP HANAバックアップでは、[Reports]ページにリダイレクトできません。

RBACの管理

SnapCenterでは、ロール、ユーザ、およびグループを変更できます。

ロールの変更

SnapCenterロールを変更して、ユーザやグループを削除したり、関連付けられている権限を変更したりできます。ロールの変更は、ロール全体で使用されている権限を変更または削除する場合に特に便利です。

開始する前に

「SnapCenterAdmin」ロールでログインする必要があります。



SnapCenter Adminロールの権限を変更または削除することはできません。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. 設定ページで、「ロール」 をクリックします。

3. 「ロール名」フィールドから、変更するロールをクリックします。
4. このロールのすべてのメンバーが他のメンバーのオブジェクトを表示できる を選択すると、ロールの他のメンバーは、リソース リストを更新した後にボリュームやホストなどのリソースを表示できるようになります。

このロールのメンバーに他のメンバーが割り当てられているオブジェクトを表示しない場合は、このオプションを選択解除します。



このオプションを有効にすると、オブジェクトまたはリソースを作成したユーザーと同じロールに属しているユーザーにオブジェクトまたはリソースへのアクセスを割り当てる必要がなくなります。

5. [Role Details]ページで、必要に応じて権限を変更するかメンバーの割り当てを解除します。
6. *送信*をクリックします。

ユーザとグループの変更

SnapCenterのユーザまたはグループを変更して、ロールやアセットを変更できます。

開始する前に

SnapCenter管理者としてログインする必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[ユーザーとアクセス]をクリックします。
3. ユーザー名またはグループ名リストから、変更するユーザーまたはグループをクリックします。
4. ユーザまたはグループの詳細ページで、ロールとアセットを変更します。
5. *送信*をクリックします。

ホストの管理

ホストの追加、SnapCenterプラグイン パッケージのインストール、検証サーバの追加、ホストの削除、バックアップ ジョブの移行、ホストの更新（プラグイン パッケージのアップグレードや新しいプラグイン パッケージの追加）などの操作を実行できます。使用するプラグインによっては、ディスクのプロビジョニング、SMB共有の管理、イニシエータ グループ (igroup) の管理、iSCSIセッションの管理、データの移行も可能です。

実行できるタスク	Microsoft Exchange Serverの場合	Microsoft SQL Serverの場合	Microsoft Windowsの場合	Oracleデータベースの場合	SAP HANAデータベースの場合	NetApp対応プラグインの場合	Db2の場合	PostgreSQLの場合	MySQLの場合
ホストの追加とプラグインパッケージのインストール	はい	はい	はい	はい	はい	はい	はい	はい	はい
ホストのESXi情報の更新	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
スケジュールの一時停止によるホストのメンテナンスモードへの切り替え	はい	はい	はい	はい	はい	はい	はい	はい	はい
プラグインの追加、アップグレード、削除によるホストの変更	はい	はい	はい	はい	はい	はい	はい	はい	はい
SnapCenterからのホストの削除	はい	はい	はい	はい	はい	はい	はい	はい	はい

実行できるタスク	Microsoft Exchange Serverの場合	Microsoft SQL Serverの場合	Microsoft Windowsの場合	Oracleデータベースの場合	SAP HANAデータベースの場合	NetApp対応プラグインの場合	Db2の場合	PostgreSQLの場合	MySQLの場合
プラグイン サービスを開始します (Windows ホストで実行されているプラグインにのみ適用されます)	はい	はい	はい	いいえ	はい	はい	はい	はい	はい
ディスクのプロビジョニング	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
SMB共有の管理	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
igroupの管理	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ
iSCSIセッションの管理	いいえ	いいえ	はい	いいえ	いいえ	いいえ	いいえ	いいえ	いいえ

仮想マシン情報の更新

VMware vCenterのクレデンシャルに変更があった場合やデータベースまたはファイルシステムのホストを再起動した場合は、仮想マシン情報を更新する必要があります。SnapCenterで仮想マシン情報を更新すると、VMware vSphere vCenterとの通信が開始され、vCenterのクレデンシャルが取得されます。



RDMベースのディスクは、データベース ホストにインストールされたSnapCenter Plug-in for Microsoft Windowsで管理されます。SnapCenter Plug-in for Microsoft Windowsは、RDMを管理するために、データベース ホストを管理するvCenterサーバと通信します。

手順

1. SnapCenter の左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。

3. [Managed Hosts]ページで、更新するホストを選択します。

4. *VM を更新*をクリックします。

プラグイン ホストの変更

プラグインのインストール後に、必要に応じてプラグイン ホストの詳細を変更できます。変更できるのは、SnapCenter Plug-in for Microsoft SQL Serverのクレデンシャル、インストール パス、プラグイン、ログディレクトリの詳細、グループ管理サービス アカウント（gMSA）、およびプラグイン ポートです。



プラグインのバージョンがSnapCenter Serverのバージョンと同じであることを確認します。

このタスクについて

- プラグイン ポートを変更できるのは、プラグインのインストール後です。

アップグレード処理の実行中は、プラグイン ポートを変更できません。

- プラグイン ポートを変更する際には、次のポートのロールバック シナリオに注意する必要があります。
 - スタンドアロン セットアップでは、SnapCenterがいずれかのコンポーネントのポート変更に失敗した場合、処理は失敗し、すべてのコンポーネントで古いポートが保持されます。

すべてのコンポーネントに関してポートが変更されたものの、いずれかのコンポーネントが新しいポートでの起動に失敗した場合、すべてのコンポーネントで古いポートが保持されます。たとえば、スタンドアロン ホスト上の2つのプラグインのポートを変更しようとして、SnapCenterがどちらかのプラグインに新しいポートを適用できなかった場合、処理は失敗し（該当するエラー メッセージが表示される）、両方のプラグインで古いポートが保持されます。

- クラスタ セットアップでは、SnapCenterがいずれかのノードにインストールされているプラグインのポート変更に失敗した場合、処理は失敗し、すべてのノードで古いポートが保持されます。

たとえば、クラスタ セットアップの4つのノードにプラグインがインストールされていて、いずれか1つのノードでポートが変更されなかった場合、すべてのノードで古いポートが保持されます。

gMSA とともにプラグインがインストールされている場合は、[その他のオプション] ウィンドウで変更できます。gMSAを使用せずにプラグインがインストールされている場合は、gMSAアカウントを指定してプラグイン サービス アカウントとして使用できます。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. 上部で*管理対象ホスト*が選択されていることを確認します。
3. 変更するホストを選択し、任意のフィールドを変更します。

一度に表示できるフィールドは1つだけです。

4. *送信*をクリックします。

結果

ホストが検証され、SnapCenter Serverに追加されます。

プラグイン サービスの起動と再起動

SnapCenterのプラグイン サービスの起動操作を行うと、サービスが実行されていない場合は起動し、サービスが実行されている場合は再起動されます。サービスの再起動は、メンテナンスの実施後などに必要になる場合があります。

サービスを再起動する場合は、ジョブが実行されていないことを確認する必要があります。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. [Managed Hosts] ページで、起動するホストを選択します。
4. クリック  アイコンをクリックし、[サービスの開始] または [サービスの再起動] をクリックします。

複数のホストのサービスを同時に起動または再起動できます。

ホスト メンテナンスのスケジュールの中断

ホストでSnapCenterのスケジュールされたジョブの実行を停止するには、ホストをメンテナンス モードにします。この操作は、プラグインをアップグレードする前、またはホストでメンテナンス タスクを実行する場合に行う必要があります。



SnapCenterは停止しているホストとは通信できないため、停止しているホストのスケジュールは中断できません。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. [管理対象ホスト] ページで、中断するホストを選択します。
4. クリック  アイコンをクリックし、[スケジュールの一時停止] をクリックして、このプラグインのホストをメンテナンス モードにします。

複数のホストのスケジュールを同時に中断できます。



プラグイン サービスを先に停止する必要はありません。プラグイン サービスが実行中でも停止した状態でも中断できます。

結果

ホスト上のスケジュールを一時停止すると、[管理対象ホスト] ページのホストの [全体ステータス] フィールドに 一時停止 と表示されます。

ホストのメンテナンスが完了したら、[スケジュールのアクティブ化] をクリックして、ホストのメンテナンス モードを終了できます。複数のホストのスケジュールを同時にアクティブ化できます。

[Resources]ページでサポートされる処理

[Resources]ページで、リソースを検出してデータ保護処理を実行できます。実行できる処理は、リソースの管理に使用しているプラグインによって異なります。

[Resources]ページで実行できるタスクは次のとおりです。

実行できるタスク	Microsoft Exchange Serverの場合	Microsoft SQL Serverの場合	Microsoft Windowsの場合	Oracleデータベースの場合	SAP HANAデータベースの場合
リソースをバックアップに使用できるかどうかの確認	はい	はい	はい	はい	はい
リソースのオンデマンド バックアップの実行	はい	はい	はい	はい	はい
バックアップからのリストア	はい	はい	はい	はい	はい
バックアップのクローニング	いいえ	はい	はい	はい	はい
バックアップの管理	はい	はい	はい	はい	はい
クローンの管理	いいえ	はい	はい	はい	はい
ポリシーの管理	はい	はい	はい	はい	はい
ストレージ接続の管理	はい	はい	はい	はい	はい
バックアップのマウント	いいえ	いいえ	いいえ	はい	いいえ
バックアップのアンマウント	いいえ	いいえ	いいえ	はい	いいえ
詳細の表示	はい	はい	はい	はい	はい

ポリシーの管理

リソースまたはリソース グループからポリシーを適用解除し、変更、削除、表示、コピーを行うことができます。

ポリシーの変更

リソースまたはリソース グループにポリシーが適用されている場合は、レプリケーションのオプション、Snapshotの保持の設定、エラーの再試行回数、またはスクリプトの情報を変更できます。スケジュールタイプ（頻度）は、ポリシーを適用解除しないと変更できません。

このタスクについて

SnapCenter Serverでは、リソースまたはリソース グループにポリシーが適用されるときにのみスケジュールタイプが登録されるため、ポリシーのスケジュール タイプを変更するには追加の手順が必要です。

状況	操作
新しいスケジュール タイプを追加	新しいポリシーを作成し、必要なリソースまたはリソース グループに適用します。 たとえば、リソース グループ ポリシーで毎時バックアップのみが指定されている場合に、日次バックアップの追加が必要となったときは、日次スケジュール タイプを設定したポリシーを作成してリソース グループに追加します。これで、リソース グループに毎時と日次の2つのポリシーが適用されます。
スケジュール タイプを削除または変更します。	次の手順を実行します。 1. 対象のポリシーを、そのポリシーを使用するすべてのリソースとリソース グループから適用解除します。 2. スケジュール タイプを変更 3. すべてのリソースとリソース グループにポリシーを適用し直します。 たとえば、ポリシーで毎時バックアップが指定されている場合に、これを日次バックアップに変更したいときは、まずポリシーを適用解除する必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定] ページで、[ポリシー] をクリックします。
3. ポリシーを選択し、[変更] をクリックします。
4. 情報を変更し、[完了] をクリックします。

ポリシーの適用解除

リソースのデータ保護を管理するポリシーが不要となった場合は、リソースまたはリソース グループからいつでもポリシーを適用解除できます。ポリシーを削除する場合やスケジュール タイプを変更する場合は、事前にポリシーを適用解除する必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。
3. リソース グループを選択し、[リソース グループの変更] をクリックします。
4. [Modify Resource Group]ウィザードの[Policies]ページに表示されるドロップダウン リストで、適用解除するポリシーの横のチェック マークをオフにします。
5. ウィザードの残りの部分でリソース グループに追加の変更を加え、[完了] をクリックします。

ポリシーの削除

不要になったポリシーは削除することができます。

開始する前に

ポリシーがリソースまたはリソース グループに関連付けられている場合は、リソースまたはリソース グループからポリシーを適用解除する必要があります。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[ポリシー]をクリックします。
3. ポリシーを選択し、[削除] をクリックします。
4. *はい*をクリックします。

リソース グループの管理

リソース グループに対してさまざまな処理を実行できます。

リソース グループに関連して次のタスクを実行できます。

- リソース グループを変更するには、リソース グループを選択し、[リソース グループの変更] をクリックして、リソース グループの作成時に指定した情報を編集します。



リソース グループを変更する際にスケジュールを変更することができます。ただし、スケジュール タイプを変更するには、ポリシーを変更する必要があります。



リソース グループからリソースを削除した場合は、リソース グループに現在適用されているポリシーに定義されたバックアップ保持の設定が、削除したリソースに引き続き適用されます。

- リソース グループのバックアップを作成する。
- バックアップのクローンを作成する。

クローニングは、SQL、Oracle、Windowsの各ファイルシステムのバックアップ、カスタム アプリケーションのバックアップ、およびSAP HANAデータベースのリソースまたはリソース グループのバックアップから実行できます。

- リソース グループのクローンを作成する。

この処理がサポートされるのは、SQLリソース グループ（データベースのみを含むもの）だけです。リソース グループのクローニングのスケジュール（クローニング ライフサイクル）を設定することができます。

- リソース グループでスケジュールされている処理が開始されないようにする。
- リソース グループを削除する。

リソース グループに対する処理の停止および再開

スケジュールされた処理を一時的に無効にして、リソース グループで開始されないように設定できます。無効にした処理は、必要に応じてあとから有効にすることができます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。
3. リソース グループを選択し、[メンテナンス] をクリックします。
4. [OK] をクリックします。

メンテナンス モードにしたリソース グループの操作を再開する場合は、リソース グループを選択し、[実稼働] をクリックします。

リソース グループの削除

リソース グループ内のリソースを保護する必要がなくなった場合は、リソース グループを削除することができます。SnapCenterからプラグインを削除する場合は、事前にリソース グループを削除する必要があります。

このタスクについて

リソース グループ内のすべてのリソースに対して作成されたすべてのクローンを手動で削除する必要があります。必要に応じて、リソース グループに関連するすべてのバックアップ、メタデータ ポリシー、およびSnapshotを強制的に削除できます。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] リストから [リソース グループ] を選択します。
3. リソース グループを選択し、[削除] をクリックします。

- オプション: リソース グループに関連付けられているすべてのバックアップ、メタデータ、ポリシー、およびスナップショットを削除するには、[このリソース グループに関連付けられているバックアップを削除し、ポリシーをデタッチする] チェック ボックスをオンにします。
- [OK]をクリックします。

バックアップの管理

バックアップは、名前変更および削除することができます。複数のバックアップを同時に削除することもできます。

バックアップの名前の変更

検索を簡単にするために、バックアップの名前を変更できます。

手順

- 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
- [リソース] ページで、[表示] ドロップダウン リストからリソースまたはリソース グループを選択します。
- リストからリソースまたはリソース グループを選択します。

リソースまたはリソース グループのトポロジ ページが表示されます。リソースまたはリソース グループがデータ保護の対象として設定されていない場合は、トポロジ ページではなく [Protect] ウィザードが表示されます。

- [コピーの管理] ビューで、プライマリ ストレージ システムから [バックアップ] を選択します。

セカンダリ ストレージ システムにあるバックアップは名前を変更できません。

Oracle Recovery Manager (RMAN) を使用して Oracle データベースのバックアップをカタログ化した場合、そのバックアップの名前は変更できません。

- バックアップを選択し、 をクリックします。
- *バックアップの名前を変更* フィールドに新しい名前を入力し、*OK* をクリックします。

バックアップの削除

別のデータ保護処理に使用する必要がなくなったバックアップは、削除することができます。

開始する前に

バックアップを削除する前に、関連付けられているクローンを削除しておく必要があります。



クローン リソースに関連付けられているバックアップは削除できません。

手順

- 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。

2. [リソース] ページで、[表示] ドロップダウン リストからリソースまたはリソース グループを選択します。
3. リストからリソースまたはリソース グループを選択します。

リソースまたはリソース グループのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリ ストレージ システムから [バックアップ] を選択します。

セカンダリ ストレージ システム上のバックアップは削除できません。

5. バックアップを選択し、 をクリックします。

SAP HANAデータベースのバックアップを削除すると、そのバックアップに関連付けられているSAP HANAカタログも削除されます。



最後に残っているバックアップが削除されると、関連付けられているHANAカタログのエントリを削除できなくなります。

6. [OK]をクリックします。



SnapCenterにあるデータベース バックアップが古くなっていて、対応するバックアップがストレージ システムにない場合は、remove-smbbackupコマンドを使用して該当する古いバックアップ エントリをクリーンアップする必要があります。この古いバックアップがカタログ化されている場合は、リカバリ カatalog データベースからカタログ化が解除されます。

保護の解除

保護を解除することによって、すべてのバックアップが削除され、すべてのポリシーが解除されます。保護を解除する前に、バックアップがマウントされておらず、バックアップにクローンが関連付けられていないことを確認する必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストからリソースまたはリソース グループを選択します。
3. リストからリソースまたはリソース グループを選択します。

リソースまたはリソース グループのトポロジ ページが表示されます。

4. バックアップを選択し、「保護の削除」をクリックします。

クローンの削除

不要と判断したクローンは削除することができます。

このタスクについて

他のクローンのソースのようにになっているクローンは削除できません。

たとえば、本番環境のデータベースがdb1であり、データベースclone1がdb1のバックアップからクローニングされ、その後、clone1が保護されます。データベースclone2がclone1のバックアップからクローニングされます。clone1を削除する場合は、まずclone2を削除してからclone1を削除する必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. [リソース] ページで、[表示] ドロップダウン リストからリソースまたはリソース グループを選択します。
3. リストからリソースまたはリソース グループを選択します。

リソースまたはリソース グループのトポロジ ページが表示されます。

4. [コピーの管理] ビューで、プライマリまたはセカンダリ (ミラーリングまたは複製) ストレージ システムから クローン を選択します。
5. クローンを選択し、 をクリックします。

SAP HANAデータベースのクローンを削除する場合は、[Delete Clone]ページで次の操作を実行します。

- a. クローン削除前 フィールドに、クローンを削除する前に実行するコマンドを入力します。
 - b. アンマウント フィールドに、クローンを削除する前にクローンをアンマウントするコマンドを入力します。
6. [OK]をクリックします。

終わったら

ファイルシステムが削除されないことがあります。次のコマンドを実行して、CLONE_DELETE_DELAY パラメータの値を増やす必要があります。./sccli Set-SmConfigSettings



CLONE_DELETE_DELAYパラメータには、アプリケーション クローンの削除が完了してからファイルシステムの削除が開始されるまでの時間を秒数で指定します。

パラメータの値を変更したら、SnapCenter Plug-in Loader (SPL) サービスを再起動します。

ジョブ、スケジュール、イベント、およびログの監視

[Monitor]ページから、ジョブの進捗状況の監視、スケジュールされたジョブに関する情報の取得、イベントやログの確認が可能です。

ジョブの監視

SnapCenterのバックアップ、クローニング、リストア、検証の各ジョブに関する情報を表示できます。このビューは、開始日と終了日、ジョブのタイプ、リソース グループ、ポリシー、またはSnapCenterプラグインでフィルタできます。また、指定したジョブの詳細情報やログ ファイルを取得することもできます。

SnapMirrorやSnapVaultの処理に関連するジョブも監視できます。



SnapCenter Adminロールまたはその他のスーパーユーザ ロールが割り当てられている場合を除き、監視できるのは自分で作成したジョブと自分に関係があるジョブだけです。

ジョブの監視に関連して次のタスクを実行できます。

- バックアップ、クローニング、リストア、検証の各処理を監視する。
- ジョブの詳細とレポートを表示する。
- スケジュールされたジョブを停止する。

スケジュールされたバックアップジョブを管理する

SnapCenter 6.0.1 リリース以降では、特定の時点で実行できるスケジュールされたジョブの数にしきい値を設定する新しいパラメーター **JobConcurrencyThreshold** が導入されました。これにより、システムのハードウェア構成に基づいて、実行するバックアップの数を制御できます。

JobConcurrencyThreshold に割り当てられているデフォルト値は 0 で、無効になっています。スケジュールされたバックアップ ウィンドウ中にパフォーマンスの低下が見られる場合、値を割り当てることで有効にすることができます。



JobConcurrencyThreshold を有効にして同時ジョブを管理すると、SnapCenterバックアップの順序を制御できなくなり、スケジュールで指定された時刻にバックアップがトリガーされない可能性があります。

手順

1. `C:\Program Files\NetApp\ SnapCenter WebApp\ SnapManager.Web.UI.dll.config` にある **JobConcurrencyThreshold** パラメータの値を設定します。
2. IIS > アプリケーション プール > SnapCenter > 再起動をクリックして、SnapCenterアプリケーション プールをリサイクルします。
3. IIS > サイト > SnapCenter > 再起動をクリックして、SnapCenter Web サービスを再起動します。

古いジョブを管理する

古いジョブは、SnapCenterでの中断や不適切なジョブ更新によって作成されます。SnapCenter 6.0.1 リリース以降では、72 時間以上停止している古いジョブをクリーンアップするための定義済みスケジュールが導入されています。設定可能なパラメータ **CleanUpStaleJobsIntervalHours** を編集することで、スケジュールの頻度を変更できます。

モニター > スケジュール > **SnapCenter_StaleJobCleanUp** からスケジュールを実行することで、オンデマンドでクリーンアップをトリガーできます。

手順

1. `C:\Program Files\NetApp\ SnapCenter WebApp\ SnapManager.Web.UI.dll.config` にある **CleanUpStaleJobsIntervalHours** パラメータの値を設定します。
2. IIS > アプリケーション プール > SnapCenter > 再起動をクリックして、SnapCenterアプリケーション プールをリサイクルします。
3. IIS > サイト > SnapCenter > 再起動をクリックして、SnapCenter Web サービスを再起動します。

スケジュールの監視

現在のスケジュールを表示して、処理の開始日時、前回の実行日時、および次回の実行日時を確認できます。また、処理が実行されるホストのほか、処理のリソース グループやポリシーに関する情報も確認できます。

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*スケジュール*をクリックします。
3. リソース グループとスケジュール タイプを選択します。
4. スケジュールされた処理の一覧を確認します。

イベントを監視する

ユーザによるリソース グループの作成、システムによるアクティビティの開始、スケジュールされたバックアップの作成など、システム内のSnapCenterイベントの一覧を表示できます。イベントを監視することで、バックアップやリストアなどの処理が実行中であるかどうかを確認することができます。

このタスクについて

[Events]ページには、すべてのジョブの情報が表示されます。たとえば、バックアップ ジョブが開始されると、「backup start」イベントが表示されます。バックアップが完了すると、「バックアップ完了」イベントが表示されます。

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. モニターページで、*イベント*をクリックします。
3. (オプション) [フィルター] ボックスに、開始日または終了日、イベントのカテゴリ (バックアップ、リソース グループ、ポリシーなど)、および重大度レベルを入力し、[適用] をクリックします。または、検索ボックスに文字を入力します。
4. イベントの一覧を確認します。

ログの監視

SnapCenter Serverログ、SnapCenterホスト エージェント ログ、およびプラグイン ログを表示およびダウンロードできます。これらのログはトラブルシューティングに役立ちます。

このタスクについて

フィルタを使用して、特定の重大度レベルのログだけを表示するように絞り込むことができます。

- デバッグ
- 情報
- 警告
- エラー
- 致命的

バックアップ ジョブが失敗した理由を特定する目的で、ジョブ レベルのログを表示することもできます。ジョブ レベルのログの場合は、[モニター]>[ジョブ] オプションを使用します。

手順

1. 左側のナビゲーション ペインで、[モニター] をクリックします。
2. 「ジョブ」 ページでジョブを選択し、「ログのダウンロード」 をクリックします。

ダウンロードされたzipフォルダには、ジョブのログと一般的なログが含まれています。zipされたフォルダの名前は、選択したジョブのIDとタイプで構成されています。

3. モニターページで、*ログ*をクリックします。
4. ログ タイプ、ホスト、およびインスタンスを選択します。

ログタイプを*プラグイン*として選択すると、ホストまたはSnapCenterプラグインを選択できます。ログタイプが*サーバー*の場合、これは選択できません。

5. 特定のソース、メッセージ、またはログ レベルでログの内容を絞り込むには、列見出しにあるフィルタアイコンをクリックします。

すべてのログを表示するには、「以上」を選択します。`Debug`レベル。

6. *更新*をクリックします。
7. ログの一覧を確認します。
8. ログをダウンロードするには、[ダウンロード] をクリックします。

ダウンロードされたzipフォルダには、ジョブのログと一般的なログが含まれています。zipされたフォルダの名前は、選択したジョブのIDとタイプで構成されています。

大規模な構成でパフォーマンスを最適化するには、PowerShellコマンドレットを使用して、SnapCenterのログ設定を最小レベルに設定します。

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10  
-JobLogsMaxFileSize 10MB -Server
```



フェイルオーバージョブの終了後に正常性または構成情報にアクセスするには、次のコマンドレットを実行します。Get-SmRepositoryConfig。

SnapCenterからのジョブとログの削除

バックアップ、リストア、クローニング、および検証の各ジョブとそのログをSnapCenterから削除することができます。SnapCenterでは、ジョブの成否にかかわらず、削除しないかぎりログは永久に保存されます。ジョブのログを削除することで、ストレージの空きを増やすことができます。

このタスクについて

実行中のジョブがないことを確認してください。ジョブIDを指定して特定のジョブを削除するか、期間を指定してその間に実行されたジョブを削除することができます。

ジョブを削除する際、ホストをメンテナンス モードに切り替える必要はありません。

手順

1. PowerShellを起動します。
2. コマンドプロンプトから次のように入力します。 `Open-SMConnection`
3. コマンドプロンプトから次のように入力します。 `Remove-SmJobs`
4. 左側のナビゲーション ペインで、[モニター] をクリックします。
5. モニターページで、*ジョブ*をクリックします。
6. [Jobs]ページで、ジョブのステータスを確認します。

関連情報

コマンドレットで使用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

SnapCenterのレポート機能の概要

SnapCenterには、システムの健全性や処理の状況を監視および管理するためのさまざまなレポート オプションが用意されています。

レポートの種類	説明
Backup Report	バックアップ レポートには、SnapCenter環境のバックアップ状況に関する全体的なデータ、バックアップの成功率、および指定した期間に実行された各バックアップに関する情報が表示されます。バックアップが削除された場合、そのバックアップのステータス情報はレポートに表示されません。バックアップ詳細レポートには、指定したバックアップ ジョブに関する詳細情報に加え、バックアップに成功したリソースと失敗したリソースの一覧が表示されます。
クローン レポート	クローン レポートには、SnapCenter環境のクローニング状況に関する全体的なデータ、クローニングの成功率、および指定した期間に実行された各クローニング ジョブに関する情報が表示されます。クローンが削除された場合、そのクローンのステータス情報はレポートに表示されません。クローン詳細レポートには、指定したクローン、クローン ホスト、クローニング ジョブ タスクのステータスについての詳細情報が表示されます。タスクが失敗した場合は、クローン詳細レポートにその情報が表示されます。

レポートの種類	説明
Restore Report	リストア レポートには、リストア ジョブに関する全体的な情報が表示されます。リストア詳細レポートには、指定したリストア ジョブについて、ホスト名、バックアップ名、ジョブの開始日時と期間、個々のジョブ タスクのステータスなどの詳細情報が表示されます。タスクが失敗した場合は、リストア詳細レポートにその情報が表示されます。
保護レポート	このレポートには、すべてのSnapCenterプラグインインスタンスで管理されているリソースについて、保護の詳細が表示されます。このレポートには、すべてのプラグイン インスタンスで管理されているリソースについて、保護の詳細が表示されます。概要に加え、保護されていないリソース、レポートの生成時にバックアップされていなかったリソース、バックアップ処理に失敗したリソース グループのリソース、およびSnapVaultステータスの詳細を確認できます。
スケジュール済みレポート	毎日、毎週、または毎月のように定期的に実行されるレポートです。指定した日時に自動的に生成され、電子メールで該当するユーザに送信されます。スケジュールは有効化、無効化、変更、または削除できます。有効にしたスケジュールは、[今すぐ実行] ボタンをクリックするとオンデマンドで実行できます。管理者はすべてのスケジュールを実行できますが、生成されるレポートに含まれるデータは、スケジュールを作成したユーザが割り当てた権限によって異なります。 管理者以外のユーザは、自分の権限に基づいてスケジュールを表示または変更できます。[Add Role] ページで[All members of this role can see other members' objects] オプションが選択されている場合、そのロールの他のメンバーは表示および変更できます。

レポートへのアクセス

SnapCenterダッシュボードを使用して、システムの健全性に関する概要を確認できます。ダッシュボードから詳細にドリルダウンできます。また、詳細レポートに直接アクセスすることもできます。

次のいずれかの方法でレポートにアクセスできます。

- 左側のナビゲーション ペインで、ダッシュボード をクリックし、最新の保護の概要 円グラフをクリックして、レポート ページで詳細を表示します。
- 左側のナビゲーション ペインで、[レポート] をクリックします。

レポートのフィルタ

必要な情報や期間に応じてパラメータを指定し、レポート データをフィルタリングできます。

手順

1. 左側のナビゲーション ペインで、[レポート] をクリックします。
2. パラメータ ビューが表示されない場合は、レポート ツールバーの [パラメータ領域の切り替え] アイコンをクリックします。
3. レポートを実行する期間を指定します。+ 終了日を省略すると、利用可能なすべての情報が取得されます。
4. 次のいずれかの条件に基づいて、レポート情報を絞り込みます。
 - リソース グループ
 - ホスト
 - ポリシー
 - リソース
 - ステータス
 - プラグイン名
5. *適用*をクリックします。

レポートのエクスポートまたは印刷

SnapCenterのレポートをエクスポートして、さまざまな形式で参照することができます。レポートは印刷することもできます。

手順

1. 左側のナビゲーション ペインで、[レポート] をクリックします。
2. レポートのツールバーから、次のいずれかを実行します。
 - 印刷可能なレポートをプレビューするには、[印刷プレビューの切り替え] アイコンをクリックします。
 - レポートを別の形式でエクスポートするには、[エクスポート] アイコンのドロップダウン リストから形式を選択します。
3. レポートを印刷するには、[印刷] アイコンをクリックします。
4. 特定のレポートの概要を確認するには、レポートの該当するセクションまでスクロールします。

Eメール通知用のSMTPサーバの設定

データ保護ジョブのレポートを自分または他のユーザに送信する際に使用するSMTPサーバを指定できます。テスト メールを送信して設定の確認することもできます。この設定は、Eメール通知を設定したSnapCenterのすべてのジョブにグローバルに適用されます。

このオプションは、すべてのデータ保護ジョブ レポートの送信に使用するSMTPサーバを設定します。ただし、特定のリソースに対するSnapCenterのデータ保護ジョブの更新情報を定期的に自分または他のユーザに

送信し、更新ステータスを監視できるようにするには、リソース グループの作成時にSnapCenterのレポートをEメールで送信するオプションを設定できます。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[グローバル設定]をクリックします。
3. SMTP サーバーを入力し、[保存] をクリックします。
4. テストメールを送信するには、メールの送信元と送信先のメールアドレスを入力し、件名を入力して、[送信] をクリックします。

レポートのEメール送信オプションの設定

SnapCenterのデータ保護ジョブの更新情報を定期的に自分または他のユーザに送信し、更新ステータスを監視できるようにするには、リソース グループの作成時にSnapCenterのレポートをEメールで送信するオプションを設定します。

開始する前に

[Settings]の[Global Settings]ページでSMTPサーバを設定しておく必要があります。

手順

1. 左側のナビゲーション ペインで [リソース] をクリックし、リストから適切なプラグインを選択します。
2. 表示するリソースの種類を選択し、[新しいリソース グループ] をクリックするか、既存のリソース グループを選択して [変更] をクリックし、既存のリソース グループの電子メール レポートを構成します。
3. [New Resource Group]ウィザードの[Notification]パネルで、レポートを常に受け取るか、障害の発生時に受け取るか、障害または警告の発生時に受け取るかをプルダウン メニューから選択します。
4. Eメールの送信元アドレス、Eメールの送信先アドレス、およびEメールの件名を入力します。

SnapCenter Serverリポジトリの管理

SnapCenterで実行したさまざまな処理に関する情報は、SnapCenter Serverデータベース リポジトリに格納されます。SnapCenter Serverをデータ損失から保護するには、リポジトリのバックアップを作成しておく必要があります。

SnapCenter Serverリポジトリは、NSMデータベースと呼ばれることもあります。

SnapCenterリポジトリを保護するための前提条件

SnapCenterリポジトリを保護するには、一定の前提条件を満たしている必要があります。

- Storage Virtual Machine (SVM) 接続の管理
ストレージのクレデンシャルを設定する必要があります。
- ホストのプロビジョニング

SnapCenterリポジトリのホストに、NetAppストレージ ディスクが少なくとも1つ必要です。
SnapCenterリポジトリのホストにNetAppディスクがない場合は作成する必要があります。

ホストの追加、SVM接続のセットアップ、およびホストのプロビジョニングの詳細については、インストール手順を参照してください。

- iSCSI LUNまたはVMDKのプロビジョニング

ハイアベイラビリティ（HA）構成の場合は、いずれかのSnapCenter ServerでiSCSI LUNまたはVMDKをプロビジョニングできます。

SnapCenterリポジトリのバックアップ

SnapCenter Serverリポジトリをバックアップすると、データ損失からの保護に役立ちます。 *Protect-SmRepository* コマンドレットを実行してリポジトリをバックアップできます。

このタスクについて

Protect-SmRepository コマンドレットは、次のタスクを実行します。

- リソース グループとポリシーを作成する
- SnapCenterリポジトリのバックアップ スケジュールを作成する

手順

1. PowerShellを起動します。
2. SnapCenter Server ホストで、 *Open-SmConnection* コマンドレットを使用してセッションを確立し、資格情報を入力します。
3. *Protect-SmRepository* コマンドレットと必要なパラメータを使用してリポジトリをバックアップします。

SnapCenterリポジトリのバックアップの表示

Get-SmRepositoryBackups コマンドレットを実行すると、 SnapCenter Server データベース リポジトリのバックアップの一覧を表示できます。

リポジトリのバックアップは、 *Protect-SmRepository* コマンドレットで指定されたスケジュールに従って作成されます。

手順

1. PowerShellを起動します。
2. コマンドプロンプトから次のコマンドレットを入力し、資格情報を入力してSnapCenterサーバーに接続します: *Open-SMConnection*
3. *Get-SmRepositoryBackups* コマンドレットを使用して、利用可能なすべてのSnapCenterデータベース バックアップを一覧表示します。

SnapCenterデータベース リポジトリのリストア

Restore-SmRepositoryBackup コマンドレットを実行して、 SnapCenterリポジトリを復元できます。

SnapCenterリポジトリのリストア中はリポジトリ データベースにアクセスできないため、SnapCenterの他の実行中の処理が影響を受けます。

手順

1. PowerShellを起動します。
2. コマンドプロンプトから次のコマンドレットを入力し、資格情報を入力してSnapCenterサーバーに接続します: *Open-SMConnection*
3. *Restore-SmRepositoryBackup* コマンドレットを使用してリポジトリのバックアップを復元します。

SnapCenterのMySQLデータベース リポジトリをiSCSI LUNまたはVMDKにある既存のバックアップからリストアするコマンドレットの例を次に示します。

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445
```

バックアップ ファイルがiSCSI LUNから誤って削除された場合にSnapCenterのMySQLデータベースをリストアするコマンドレットの例を次に示します。VMDK の場合は、ONTAPスナップショットからバックアップを手動で復元します。

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```



リポジトリのリストア処理に使用されたバックアップは、リストア処理の実行後にリポジトリのバックアップが取得されると、リストに表示されなくなります。

SnapCenterリポジトリの移行

SnapCenter Serverデータベース リポジトリをデフォルトの場所から別のディスクに移行することができます。リポジトリの移行は、よりスペースが多いディスクに再配置する場合などに行います。

手順

1. WindowsでMySQL57サービスを停止します。
2. MySQLのデータ ディレクトリを探します。

通常、データ ディレクトリは、C:\ProgramData\MySQL\MySQL Server 5.7\Dataにあります。

3. MySQLのデータ ディレクトリを新しい場所（例：E:\Data\nsm）にコピーします。
4. 新しいディレクトリを右クリックし、[プロパティ]>[セキュリティ]を選択して、ネットワーク サービス ローカル サーバー アカウントを新しいディレクトリに追加し、アカウントにフル コントロールを割り当てます。
5. 元のデータベース ディレクトリの名前を変更します（例：nsm_copy）。
6. Windows コマンド プロンプトから、*mklink* コマンドを使用してシンボリック ディレクトリ リンクを作成します。

```
"mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
```

7. WindowsでMySQL57サービスを開始します。
8. SnapCenterにログインしてリポジトリのエントリを確認するか、MySQLユーティリティにログインして新しいリポジトリに接続して、データベースの場所が正しく変更されたことを確認します。
9. 名前を変更した元のデータベース リポジトリ ディレクトリ (nsm_copy) を削除します。

SnapCenterリポジトリのパスワードのリセット

MySQL Serverリポジトリ データベースのパスワードは、SnapCenter 4.2からSnapCenter Serverをインストールする際に自動的に生成されます。SnapCenterユーザはこの自動生成されたパスワードを確認することはできません。リポジトリ データベースにアクセスするには、パスワードをリセットする必要があります。

開始する前に

パスワードをリセットするためには、SnapCenterの管理者権限が必要です。

手順

1. PowerShellを起動します。
2. コマンドプロンプトから次のコマンドを入力し、 SnapCenter Server に接続するための資格情報を入力します: *Open-SMConnection*
3. リポジトリのパスワードをリセットします: *Set-SmRepositoryPassword*

リポジトリ パスワードをリセットするコマンドの例を次に示します。

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: *****
ConfirmPassword: *****
Successfully updated the MySQL server password.
```

関連情報

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

信頼されていないドメインのリソースの管理

SnapCenterは、Active Directory (AD) の信頼されたドメインのホストに加え、信頼されていない複数のADドメインのホストも管理します。信頼されていないADドメインをSnapCenter Serverに登録しておく必要があります。SnapCenterでは、信頼されていない複数のADドメインのユーザとグループがサポートされます。

SnapCenter Serverは、ドメインまたはワークグループのいずれかに属するマシンにインストールできます。SnapCenter Serverをインストールするには、ドメインに属するマシンの場合はドメインのクレデンシャル、ワークグループに属するマシンの場合はローカル管理者のクレデンシャルを指定する必要があります。

SnapCenter Serverに登録されていないドメインに属するActive Directory (AD) グループはサポートされません。これらの AD グループを使用してSnapCenterロールを作成することはできますが、 SnapCenter Server へのログインは失敗し、次のエラー メッセージが表示されます: ログインしようとしているユーザーは、どのロールにも属していません。管理者に問い合わせてください。」というエラー メッセージが表示されます。

信頼されていないドメインの変更

信頼されていないドメインを変更し、ドメイン コントローラのIPアドレスや完全修飾ドメイン名 (FQDN) を変更できます。

このタスクについて

FQDNを変更すると、関連付けられているアセット (ホスト、ユーザ、グループ) が想定どおりに機能しなくなる場合があります。

信頼されていないドメインの変更には、SnapCenterユーザ インターフェイスまたはPowerShellコマンドレットを使用できます。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定]ページで、[グローバル設定]をクリックします。
3. [グローバル設定]ページで、[ドメイン設定]をクリックします。

4.  をクリックし、次の詳細を入力します。

フィールド	操作
ドメインFQDN	FQDN を指定し、[解決] をクリックします。
ドメインコントローラのIPアドレス	ドメインのFQDNを解決できない場合、ドメイン コントローラのIPアドレスを1つ以上指定します。

5. [OK]をクリックします。

信頼されていないActive Directoryドメインの登録解除

信頼されていないActive Directoryドメインに関連付けられているアセットを使用しない場合、そのドメインの登録を解除できます。

開始する前に

信頼されていないドメインに関連付けられているホスト、ユーザ、グループ、およびクレデンシャルを削除しておく必要があります。

このタスクについて

- SnapCenter Serverから登録を解除したドメインのユーザはSnapCenter Serverにアクセスできなくなります。

- ドメインの登録を解除すると、関連付けられているアセット（ホスト、ユーザ、およびグループ）は操作できなくなります。
- 信頼されていないドメインの登録解除には、SnapCenterユーザ インターフェイスまたはPowerShellコマンドレットを使用できます。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. [設定] ページで、[グローバル設定] をクリックします。
3. [グローバル設定] ページで、[ドメイン設定] をクリックします。
4. ドメインのリストから、登録解除するドメインを選択します。
5. クリック  をクリックし、[OK] をクリックします。

ストレージ システムの管理

ストレージ システムを追加したあと、ストレージ システムの設定や接続を変更したり、ストレージ システムを削除したりできます。

ストレージ システムの設定の変更

SnapCenterを使用してストレージ システムの設定を変更し、ユーザ名、パスワード、プラットフォーム、ポート、プロトコル、タイムアウト時間、優先IPアドレス、メッセージングの各オプションを変更することができます。

このタスクについて

個々のユーザまたはグループのストレージ接続を変更できます。あるユーザが同じストレージ システムへの権限が付与された複数のグループに所属している場合、ストレージ接続リストにはそのストレージ接続の名前が重複して（権限が割り当てられているグループごとに）表示されます。

手順

1. 左側のナビゲーション ペインで、[ストレージ システム] をクリックします。
2. [ストレージ システム] ページの [タイプ] ドロップダウンから、次のいずれかのアクションを実行します。

選択するオプション	手順
ONTAP SVM	追加されたすべてのStorage Virtual Machine (SVM) を表示し、目的のSVM設定を変更するには、次の手順を実行します。 [Storage Connections]ページで、該当するSVMの名前をクリックします。 - 次のいずれかを実行します。 - SVM がどのクラスタにも属していない場合は、[ストレージ システムの変更] ページで、ユーザー名、パスワード、EMS およびAutoSupport設定、プラットフォーム、プロトコル、ポート、タイムアウト、優先 IP などの構成を変更します。 - SVM がクラスタの一部である場合は、[ストレージ システムの変更] ページで [SVM を個別に管理] を選択し、ユーザー名、パスワード、EMS およびAutoSupport設定、プラットフォーム、プロトコル、ポート、タイムアウト、優先 IP などの構成を変更します。 SVM を独立して管理できるように変更した後、クラスター経由で管理することにした場合は、SVM を削除して [再検出] をクリックする必要があります。SVMがONTAPクラスタに追加されます。  SnapCenter GUIでストレージ システムのパスワードを更新した場合、該当するプラグインまたはサーバ ホストのSMCoreサービスを再起動する必要があります。再起動しないと、更新したパスワードがSMCoreに反映されないため、クレデンシャル エラーでバックアップ ジョブが失敗します。

選択するオプション	手順
ONTAP クラスタ	追加されたすべてのクラスタを表示し、目的のクラスタ設定を変更するには、次の手順を実行します。 [Storage Connections] ページで、クラスタの名前をクリックします。 [Modify Storage System] ページで、[Username] の横の編集アイコンをクリックし、ユーザ名とパスワードを変更します。 - EMS および AutoSupport の設定を選択または選択解除します。 *その他のオプション* をクリックし、プラットフォーム、プロトコル、ポート、タイムアウト、優先 IP などのその他の構成を変更します。

3. *送信* をクリックします。

ストレージ システムの削除

SnapCenter を使用して、使用していないストレージ システムを削除できます。

このタスクについて

個々のユーザまたはグループのストレージ接続を削除できます。あるユーザが同じストレージ システムへの権限が付与された複数のグループに所属している場合、ストレージ接続リストにはそのストレージ システムの名前が重複して（権限が割り当てられているグループごとに）表示されます。



ストレージ システムを削除すると、そのストレージ システムで実行中の処理はすべて失敗します。

手順

1. 左側のナビゲーション ペインで、[ストレージ システム] をクリックします。
2. [ストレージ システム] ページの [タイプ] ドロップダウンから、[ONTAP SVM] または [ONTAP クラスタ] を選択します。
3. [Storage Connections] ページで、削除する SVM または クラスタの横にあるチェック ボックスを選択します。



クラスタに含まれる SVM は選択できません。

4. *削除* をクリックします。
5. ストレージ システム接続設定の削除ページで、[OK] をクリックします。



ONTAP GUI を使用して ONTAP クラスタから SVM が削除された場合は、SnapCenter GUI で [再検出] をクリックして SVM リストを更新します。

REST APIサポート

ONTAPへのすべてのASA、AFF、またはFASシステム接続は、デフォルトで ZAPI を経由します。REST API は特定のONTAPバージョンに対して有効にできます。

SnapCenter は、ZAPI をサポートしていないASA r2 システム上のすべての操作を REST API を利用して実行します。

次の構成ファイル内の構成キーを変更できます。

- ストレージ接続のRestEnabled

デフォルト値は false です。

- 使用する最小オンタップバージョンREST

デフォルト値は 9.13.1 です。

REST API 経由で接続を有効にする

1. IsRestEnabledForStorageConnection を true に設定します。
2. サーバーおよび Windows プラグイン ホストの両方で、SMCoreServiceHost.dll.config および SnapDriveService.dll.config にキーを追加します。

<キーを追加="IsRestEnabledForStorageConnection" 値="true" />

REST API 経由の接続を特定バージョンのONTAPに制限する

1. 構成パラメータ MinOntapVersionToUseREST を true に設定します。
2. サーバーおよび Windows プラグイン ホストの両方で、SMCoreServiceHost.dll.config および SnapDriveService.dll.config にキーを追加します。

<キーを追加="MinOntapVersionToUseREST" 値="9.13.1" />

3. サーバー上の SmCore サービスと、プラグイン マシン上のプラグインおよびSnapDriveサービスを再起動します。

EMSデータ収集の管理

イベント管理システム（EMS）のデータ収集は、PowerShellコマンドレットを使用してスケジュール設定および管理できます。EMSデータ収集では、SnapCenter Server、インストールされているSnapCenterプラグイン パッケージ、ホストに関する情報などが収集され、指定したONTAP Storage Virtual Machine（SVM）に送信されます。



データ収集タスクの実行中はシステムのCPU利用率が上昇します。CPU利用率は、データ サイズに関係なく、処理の実行中は高いままです。

EMSデータ収集の停止

EMSデータ収集は、デフォルトで有効になり、インストールした日から7日ごとに実行されます。PowerShell コマンドレット *Disable-SmDataCollectionEMS* を使用すると、いつでもデータ収集を無効にすることができます。

手順

1. PowerShell コマンド ラインから、「*Open-SmConnection*」と入力して、SnapCenterとのセッションを確立します。
2. *Disable-SmDataCollectionEms* と入力して EMS データ収集を無効にします。

EMSデータ収集の開始

EMSデータ収集はデフォルトで有効になっており、インストールした日から7日ごとに実行するようにスケジュールされています。無効にした場合は、*Enable-SmDataCollectionEMS* コマンドレットを使用して EMS データ収集を再度開始できます。

NetApp ONTAPイベント generate-autosupport-log 権限がストレージ仮想マシン (SVM) ユーザーに付与されました。

手順

1. PowerShell コマンド ラインから、「*Open-SmConnection*」と入力して、SnapCenterとのセッションを確立します。
2. *Enable-SmDataCollectionEMS* と入力して EMS データ収集を有効にします。

EMSデータ収集のスケジュールとターゲットSVMの変更

PowerShellコマンドレットを使用して、EMSデータ収集のスケジュールやターゲットStorage Virtual Machine (SVM) を変更することができます。

手順

1. PowerShell コマンド ラインからSnapCenterとのセッションを確立するには、*Open-SmConnection* コマンドレットを入力します。
2. EMS データ収集ターゲットを変更するには、*Set-SmDataCollectionEmsTarget* コマンドレットを入力します。
3. EMS データ収集スケジュールを変更するには、*Set-SmDataCollectionEmsSchedule* コマンドレットを入力します。

EMSデータ収集のステータス監視

複数のPowerShellコマンドレットを使用して、EMSデータ収集のステータスを監視できます。スケジュール、Storage Virtual Machine (SVM) ターゲット、およびステータスに関する情報を取得することができます。

手順

1. PowerShell コマンド ラインから、「*Open-SmConnection*」と入力して、SnapCenterとのセッションを確立します。
2. *Get-SmDataCollectionEmsSchedule* と入力して、EMS データ収集スケジュールに関する情報を取得しま

す。

3. `Get-SmDataCollectionEmsStatus` と入力して、EMS データ収集ステータスに関する情報を取得します。
4. `Get-SmDataCollectionEmsTarget` と入力して、EMS データ収集ターゲットに関する情報を取得します。

関連情報

コマンドレットで利用できるパラメータとその説明に関する情報は、`Get-Help command_name` を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

SnapCenter Serverとプラグインのアップグレード

利用可能なアップデートを確認するためのSnapCenterの設定

SnapCenterは、NetAppサポート サイトと定期的に通信し、利用可能なソフトウェア アップデートがあればユーザに通知します。スケジュールを作成し、利用可能なアップデートに関する情報の受信間隔を指定することもできます。

手順

1. 左側のナビゲーション ペインで、[設定] をクリックします。
2. *設定*ページで、*ソフトウェア*をクリックします。

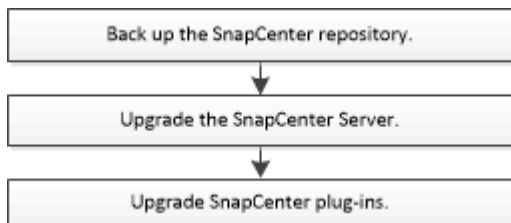
[Available Software]ページには、利用可能なプラグイン パッケージ、利用可能なバージョン、およびインストールのステータスが表示されます。

3. 更新を確認 をクリックして、プラグイン パッケージの新しいバージョンが利用可能かどうかを確認します。
4. [更新のスケジュール] をクリックしてスケジュールを作成し、利用可能な更新に関する情報を受信する間隔を指定します。
 - a. *更新の確認*で間隔を選択します。
 - b. SnapCenter Server Admin Windows 資格情報を選択し、[OK] をクリックします。

アップグレード ワークフロー

SnapCenterの各リリースには、更新されたSnapCenter Serverおよびプラグイン パッケージが含まれています。プラグイン パッケージのアップデートは、SnapCenterインストーラと一緒に配布されます。利用可能なアップデートを確認するようにSnapCenterを設定できます。

このワークフローは、SnapCenter Serverとプラグイン パッケージのアップグレードに必要な各種のタスクを示しています。



サポートされているアップグレード パス

アップグレード パスは、以前のすべてのバージョンのSnapCenterから最新バージョンのSnapCenterにアップグレードできるかどうか、およびサポートされているプラグインのバージョンを把握するのに役立ちます。

SnapCenter Serverのバージョン	SnapCenter Serverを直接アップグレードできる環境	サポートされているプラグインのバージョン
5.0	6.0	• 5.0 • 6.0
	6.0.1	• 6.0.1
	6.1	• 6.1
6.0	6.0.1	• 6.0 • 6.0.1
	6.1	• 6.1
6.0.1	6.1	• 6.0.1 • 6.1

SnapCenter Plug-in for VMware vSphere のアップグレードについては、以下を参照してください。
["SnapCenter Plug-in for VMware vSphereのアップグレード"](#)。

WindowsホストでのSnapCenter Serverのアップグレード

最新バージョンで提供される最新の機能と拡張機能にアクセスするには、SnapCenter Server をアップグレードする必要があります。

開始する前に

- SnapCenter Server ホストを最新の Windows 更新プログラムで更新し、保留中のシステム再起動がないことを確認します。
- アップグレードを開始する前に、他の操作が実行されていないことを確認してください。
- ASP.NET Core ランタイム 8.0.12 (およびそれ以降のすべての 8.0.x パッチ) ホスティング バンドルと PowerShell 7.4.2 以降をインストールします。
- ジョブが実行されていないことを確認した後、SnapCenterリポジトリ (MySQL) データベースをバックアップします。SnapCenter ServerとExchangeプラグインをアップグレードする前に、これを行っておくことが推奨されます。

詳細については、["SnapCenterリポジトリのバックアップ"](#)。

- SnapCenter Server ホストまたはプラグイン ホストで変更したすべてのSnapCenter構成ファイルをバックアップします。

SnapCenter構成ファイルの例: SnapDriveService.exe.config、SMCoreServiceHost.exe.config など。

- SnapCenter 5.0 に複数のバージョンのカスタム プラグインをインストールしている場合は、6.0 以降にアップグレードする前に、PowerShell コマンドレットを実行して、以前のバージョンのカスタム プラグイ

ン (最新バージョンを除く) をすべて SnapCenter リポジトリ (NSM データベース) から削除する必要があります。

- 走る `Open-SmConnection` SnapCenter Admin ロールの資格情報を使用してログインします
- 走る `Remove-SmPluginPackage -PluginName M<plug-in name> -PluginVersion <version number>`

```
https://kb.netapp.com/data-  
mgmt/SnapCenter/SC_KBs/SnapCenter_6.0_upgrade_fails_in_nsm_repository  
_upgrade_SQL_script_8["SnapCenter 6.0以降へのアップグレードが失敗する"]。
```

タスク概要

- アップグレード中に、SnapCenter は SQL スクリプトを実行して NSM データベース内の Exchange データを更新し、DAG とホストの短縮名を FQDN に変換します。これは、Exchange プラグインとともに SnapCenter Server を使用する場合にのみ適用されます。
- サーバー ホストを手動でメンテナンス モードにした場合は、アップグレード後に ホスト > スケジュールのアクティブ化を選択して、サーバー ホストのメンテナンス モードを解除します。
- ポリシーでプリスクリプトとポストスクリプトを有効にしている既存のバックアップ スケジュールと検証スケジュールについては、アップグレード後もバックアップ処理は引き続き機能します。

ジョブの詳細 ページでは、スクリプトを SCRIPTS_PATH にコピーし、ポリシーを編集して SCRIPTS_PATH を基準としたパスを指定することを推奨する警告メッセージが表示されます。クローン ライフサイクル ジョブについては、サブジョブ レベルで警告メッセージが表示されます。

手順

1. SnapCenter Server のインストール パッケージを NetApp サポート サイトからダウンロードします。

<https://mysupport.netapp.com/site/products/all/details/snapcenter/downloads-tab>

2. C:\Program Files\NetApp\SnapCenter WebAppにある web.config のコピーを作成します。
3. アップグレードが失敗した場合に復元できるように、Windows タスク スケジューラから SnapCenter プラグイン ホスト スケジュールをエクスポートします。

```
md d:\SCBackup\`schtasks /query /xml /TN taskname >>  
"D:\SCBackup\taskname.xml"
```

4. リポジトリのバックアップが設定されていない場合は、SnapCenter MySQL データベース ダンプを作成します。

```
md d:\SCBackup\`mysqldump --all-databases --single-transaction --add-drop  
-database --triggers --routines --events -u root -p >  
D:\SCBackup\SCRepoBackup.dmp
```

プロンプトが表示されたら、パスワードを入力します。

5. ダウンロードした .exe ファイルをダブルクリックして、SnapCenter Server のアップグレードを開始します。

アップグレードを開始すると、SnapCenter は事前チェックを実行します。システムが最小要件を満たしていない場合、SnapCenter はエラーまたは警告メッセージを表示します。警告を無視してインストールを続行できますが、エラーがあれば修正する必要があります。



SnapCenter は、以前のバージョンの SnapCenter Server のインストール時に提供された既存の MySQL Server リポジトリ データベース パスワードを引き続き使用します。

6. *アップグレード*を選択します。

どの段階でも「キャンセル」を選択すると、SnapCenter はアップグレードを停止します。キャンセルしても SnapCenter Server は以前の状態にロールバックされません。

ベスト プラクティス: ログアウトして再度ログインするか、新しいブラウザを開いて SnapCenter ユーザー インターフェイスにアクセスします。

終了後の操作

- プラグインが sudo ユーザーを使用してインストールされている場合は、`C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` にある sha224 キーをコピーして、`/etc/sudoers` ファイルを更新する必要があります。
- サーバー ホスト上のリソースの新規検出を実行する必要があります。

SnapCenter にサーバ ホストのステータスが停止として表示される場合は、しばらく待ってから新規検出を実行してください。**HostRefreshInterval** パラメータの値 (デフォルト値は 3600 秒) を 10 分を超える任意の値に変更することもできます。

- アップグレードが失敗した場合は、失敗したインストールをクリーンアップし、以前のバージョンの SnapCenter を再インストールして、NSM データベースを以前の状態に復元します。
- サーバー ホストをアップグレードした後、ストレージ システムを追加する前にプラグインもアップグレードする必要があります。

Linux ホストでの SnapCenter Server のアップグレード

SnapCenter Server インストーラ ファイルを使用して、SnapCenter Server をアップグレードできます。

手順

1. いずれかの操作を実行して、SnapCenter Server をアップグレードします。

実行する処理	操作
非対話型アップグレード	<pre>sudo ./snapcenter-linux-server- (e18/e19/sles15).bin -i silent -DUPGRADE=<value> -DINSTALL_LOG_NAME=<filename></pre> 例：sudo ./snapcenter_linux_server.bin -i silent -DUPGRADE=1 -DINSTALL_LOG_NAME=InstallerLog.log ログは <i>/var/opt/snapcenter/logs</i> に保存されます。 アップグレードするために渡すパラメータ： • DINSTALL_LOG_NAME: インストール ログが保存されるログ ファイル名。 • DUPGRADE: デフォルト値は 0 です。SnapCenter Serverをアップグレードするには、このパラメータに0以外の任意の整数を指定します。
対話型インストール	<pre>./snapcenter-linux-server- (e18/e19/sles15).bin</pre> アップグレードの確認を求められます。SnapCenter Serverのアップグレードを確認するには、0以外の値を入力します。



SnapCenter GUIにアクセスするには、SnapCenterからログアウトしてログインし直すか、ブラウザを閉じてから新しく開き直す必要があります。

プラグイン パッケージのアップグレード

プラグイン パッケージは、SnapCenterアップグレードと一緒に配布されます。

アップグレード手順によって Windows、Linux、または AIX プラグイン ホストがメンテナンス モードになるため、アップグレードする各プラグイン ホストを手動でメンテナンス モードにする必要はありません。メンテナンス モードでは、アップグレード中にプラグイン ホスト上でスケジュールされたジョブが実行されないようにします。

開始する前に

- Linux マシンにアクセスできる非 root ユーザーの場合は、アップグレード操作を実行する前に、*/etc/sudoers* ファイルを最新のチェックサム値で更新する必要があります。
- SnapCenterはデフォルトで環境からJAVA_HOMEを検出します。固定の JAVA_HOME を使用し、Linux ホスト上のプラグインをアップグレードする場合は、*/var/opt/snapcenter/spl/etc/* にある *spl.properties* ファイルに SKIP_JAVAHOME_UPDATE パラメータを手動で追加し、値を TRUE に設定する必要があります。

JAVA_HOMEの値は、プラグインがアップグレードされたとき、またはSnapCenter Plug-in Loader (SPL) サービスが再起動されたときに更新されます。SPLをアップグレードまたは再起動する前に、SKIP_JAVAHOME_UPDATEパラメータを追加して値をTRUEに設定すると、JAVA_HOMEの値は更新されません。

- SnapCenter Serverホストまたはプラグイン ホストで変更したSnapCenter構成ファイルをすべてバックアップしておく必要があります。

SnapCenter構成ファイルの例: SnapDriveService.exe.config、SMCoreServiceHost.exe.config など。

タスク概要

- SnapCenter Plug-in for Microsoft SQL Server、SnapCenter Plug-in for Microsoft Exchange Server、SnapCenter Plug-in for Microsoft Windowsでは、SCRIPTS_PATHを実行するために、サーバとプラグイン ホストの両方を最新バージョンにアップグレードすることが推奨されます。

ポリシーでプリスクリプトとポストスクリプトを有効にしている既存のバックアップ スケジュールと検証スケジュールについては、アップグレード後もバックアップ処理は引き続き機能します。

ジョブの詳細 ページでは、スクリプトを SCRIPTS_PATH にコピーし、ポリシーを編集してSCRIPTS_PATH を基準としたパスを指定することを推奨する警告メッセージが表示されます。クローンライフサイクル ジョブについては、サブジョブ レベルで警告メッセージが表示されます。

手順

1. 左側のナビゲーション ペインで、ホスト > 管理対象ホスト をクリックします。
2. 次のいずれかのタスクを実行して、ホストをアップグレードします。
 - いずれかのプラグインホストの「全体ステータス」列に「アップグレード可能」と表示される場合は、プラグインホスト名をクリックして、次の操作を実行します。
 - i. *その他のオプション*をクリックします。
 - ii. プラグイン ホストがプラグインをアップグレードするための要件を満たしているかどうかを検証しない場合は、事前チェックをスキップ を選択します。
 - iii. *アップグレード*をクリックします。
 - 複数のホストをアップグレードする場合は、すべてのホストを選択し、 をクリックし、[アップグレード] > [OK] をクリックします。

関連するサービスはすべてプラグインのアップグレード中に再起動されます。



パッケージ内のすべてのプラグインが選択されますが、以前のバージョンのSnapCenterでインストールされたプラグインのみがアップグレードされ、それ以外のプラグインはインストールされません。新しいプラグインをインストールするには、「プラグインの追加」オプションを使用する必要があります。

「事前チェックをスキップ」チェックボックスを選択していない場合、プラグインホストがプラグインのインストール要件を満たしているかどうかを検証されます。最小要件を満たしていない場合は、適切なエラーメッセージまたは警告メッセージが表示されます。問題を修正したら、「アップグレード」をクリックします。



エラーがディスク スペースまたはRAMに関連している場合は、C:\Program Files\NetApp\SnapCenter WebAppにあるweb.configまたはC:\Windows\System32\WindowsPowerShell\v1.0\Modules\SnapCenter\にあるPowerShell構成ファイルを更新して、デフォルト値を変更してください。エラーがそれ以外のパラメータに関連している場合は、問題を修正してから要件を再度検証する必要があります。

機器更改

SnapCenter Serverホストの機器更改

SnapCenter Serverホストの更改が必要な場合は、同じバージョンのSnapCenter Serverを新しいホストにインストールし、APIを実行して古いサーバからSnapCenterをバックアップして、新しいサーバでリストアできます。

手順

1. 新しいホストを導入し、次のタスクを実行します。
 - a. 同じバージョンのSnapCenter Serverをインストールします。
 - b. (オプション) CA証明書を設定し、双方向SSLを有効にします。詳細については、["CA証明書の設定"](#)そして["双方向SSLを設定して有効にする"](#)。
 - c. (オプション) 多要素認証を設定します。["多要素認証を有効にする"](#)。
2. SnapCenter Adminユーザとしてログインします。
3. 次のいずれかの API を使用して、古いホスト上のSnapCenter Server のバックアップを作成します。
``/<snapcenter_version>/server/backup``またはコマンドレット: *New-SmServerBackup*。



バックアップを作成する前に、スケジュールされたすべてのジョブを一時停止し、実行中のジョブがないことを確認します。



新しいドメインで実行されているSnapCenter Serverでバックアップをリストアする場合は、バックアップを作成する前に、古いSnapCenterホストに新しいドメイン ユーザを追加し、SnapCenter Adminロールを割り当てる必要があります。

4. 古いホストから新しいホストにバックアップをコピーします。
5. 次のいずれかの API を使用して、新しいホストでSnapCenter Server のバックアップを復元します。
``/<snapcenter_version>/server/restore``またはコマンドレット: *Restore-SmServerBackup*。

デフォルトでは、リストアによって、すべてのホストでSnapCenter Server URLが新しいものに更新されます。更新をスキップする場合は、`-SkipSMSURLInHosts` 属性を使用し、次のいずれかの API を使用してサーバー URL を個別に更新します。 ``/<snapcenter_version>/server/configureurl``またはコマンドレット: *Set-SmServerConfig*。



プラグイン ホストがサーバー ホスト名を解決できない場合は、各プラグイン ホストにログインし、`<新しい IP> SC_Server_Name` 形式で新しい IP の `etc/host` エントリを追加します。



サーバーの `etc/host` エントリは復元されません。古いサーバから手動でリストアできません。

新しいドメインで実行されているSnapCenter Serverにバックアップをリストアする場合に、古いドメイン ユーザを引き続き使用するには、古いドメインを新しいSnapCenter Serverに登録する必要があります。



古いSnapCenterホストでweb.configファイルを手動で更新した場合、その更新内容は新しいホストにコピーされません。新しいホストのweb.configファイルでも、同じ変更を手動で行う必要があります。

6. SnapCenter Server URL の更新をスキップした場合、または復元プロセス中にいずれかのホストがダウンしていた場合は、次のいずれかの API を使用して、SnapCenterによって管理されているすべてのホストまたは指定されたホストで新しいサーバ名を更新します。`<snapcenter\_version>/server/configureurl` またはコマンドレット: *Set-SmServerConfig*。
7. 新しいSnapCenter Serverからすべてのホストのスケジュール済みジョブをアクティブ化します。

F5クラスタ内のノードの機器更改

F5クラスタ内のノードを削除して新しいノードを追加することで、ノードの機器更改を実行できます。機器更改が必要なノードがアクティブな場合は、クラスタの別のノードをアクティブにしてからノードを削除します。

F5クラスタにノードを追加する方法については、以下を参照してください。 ["F5を使用したSnapCenter Serverの高可用性の設定"](#)。



F5 クラスターの URL が変更された場合は、次のいずれかの API を使用してすべてのホストで URL を更新できます。`<snapcenter\_version>/server/configureurl` またはコマンドレット: *Set-SmServerConfig*。

古いSnapCenter Serverホストの運用停止

新しいSnapCenter Serverが稼働中であることと、すべてのプラグイン ホストが新しいSnapCenter Serverホストと通信できることを確認したら、古いSnapCenter Serverホストを削除できます。

古いSnapCenter Serverホストへのロールバック

問題が発生した場合は、次のいずれかの API を使用してすべてのホストのSnapCenter Server URL を更新することで、古いSnapCenter Server ホストを復元できます。`<snapcenter\_version>/server/configureurl` またはコマンドレット: *Set-SmServerConfig*。

ディザスタ リカバリ

スタンドアロンSnapCenterホストのディザスタ リカバリ

サーバのバックアップを新しいホストにリストアすることで、ディザスタ リカバリを実行できます。

開始する前に

古いSnapCenter Serverのバックアップがあることを確認します。

手順

1. 新しいホストを導入し、次のタスクを実行します。
 - a. 同じバージョンのSnapCenter Serverをインストールします。
 - b. CA証明書を設定し、双方向SSLを有効にします。詳細については、["CA証明書の設定"](#)そして ["双方向SSLを設定して有効にする"](#)。

2. 古いSnapCenter Serverのバックアップを新しいホストにコピーします。
3. SnapCenter Adminユーザとしてログインします。
4. 次のいずれかの API を使用して、新しいホストでSnapCenter Server のバックアップを復元します。
`/<snapcenter\_version>/server/restore` または コマンドレット: *Restore-SmServerBackup*。

デフォルトでは、リストアによって、すべてのホストでSnapCenter Server URLが新しいものに更新されます。更新をスキップする場合は、*-SkipSMSURLInHosts* 属性を使用し、次のいずれかの API を使用してサーバー URL を個別に更新します。`/<snapcenter\_version>/server/configureurl` または コマンドレット: *Set-SmServerConfig*。



プラグイン ホストがサーバー ホスト名を解決できない場合は、各プラグイン ホストにログインし、<新しい IP> SC_Server_Name 形式で新しい IP の *etc/host* エントリを追加します。



サーバーの *etc/host* エントリは復元されません。古いサーバから手動でリストアできます。

5. URL の更新をスキップした場合、または復元プロセス中にいずれかのホストがダウンしていた場合は、次のいずれかの API を使用して、SnapCenterによって管理されているすべてのホストまたは指定されたホストで新しいサーバー名を更新します。`/<snapcenter\_version>/server/configureurl` または コマンドレット: *Set-SmServerConfig*。

SnapCenter F5クラスタのディザスタ リカバリ

サーバのバックアップを新しいホストにリストアし、スタンドアロン ホストをクラスタに変換することで、ディザスタ リカバリを実行できます。

開始する前に

古いSnapCenter Serverのバックアップがあることを確認します。

手順

1. 新しいホストを導入し、次のタスクを実行します。
 - a. 同じバージョンのSnapCenter Serverをインストールします。
 - b. CA証明書を設定し、双方向SSLを有効にします。詳細については、["CA証明書の設定"](#)そして ["双方向SSLを設定して有効にする"](#)。
2. 古いSnapCenter Serverのバックアップを新しいホストにコピーします。
3. SnapCenter Adminユーザとしてログインします。
4. 次のいずれかの API を使用して、新しいホストでSnapCenter Server のバックアップを復元します。
`/<snapcenter\_version>/server/restore` または コマンドレット: *Restore-SmServerBackup*。

デフォルトでは、リストアによって、すべてのホストでSnapCenter Server URLが新しいものに更新されます。更新をスキップする場合は、*-SkipSMSURLInHosts* 属性を使用し、次のいずれかの API を使用してサーバー URL を個別に更新します。`/<snapcenter\_version>/server/configureurl` または コマンドレット: *Set-SmServerConfig*。



プラグイン ホストがサーバー ホスト名を解決できない場合は、各プラグイン ホストにログインし、<新しい IP> SC_Server_Name 形式で新しい IP の *etc/host* エントリを追加します。



サーバーの *etc/host* エントリは復元されません。古いサーバから手動でリストアできません。

- URL の更新をスキップした場合、または復元プロセス中にいずれかのホストがダウンしていた場合は、次のいずれかの API を使用して、SnapCenterによって管理されているすべてのホストまたは指定されたホストで新しいサーバー名を更新します。`<snapcenter\_version>/server/configureurl` またはコマンドレット: *Set-SmServerConfig*。
- スタンドアロン ホストをF5クラスタに変換します。

F5の設定方法については、"[F5を使用したSnapCenter Serverの高可用性の設定](#)"。

関連情報

APIに関する情報については、Swaggerページにアクセスする必要があります。"[Swagger API Webページを使用してREST APIにアクセスする方法](#)"。

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

SnapCenterプラグイン ホストの機器更改

SnapCenterプラグイン ホストの機器更改が必要な場合は、古いホストから新しいホストにリソースを移動する必要があります。新しいホストをSnapCenterに追加すると、すべてのリソースが検出されますが、それらは新しいリソースとして扱われます。

タスク概要

古いホスト名と新しいホスト名を入力として受け取るAPIまたはコマンドレットを実行し、リソースを名前と比較して、一致するリソースのオブジェクトを古いホストから新しいホストに再リンクする必要があります。一致するリソースは保護対象としてマークされます。

- IsDryRun* パラメータはデフォルトで True に設定されており、これにより古いホストと新しいホストの一致するリソースが識別されます。

一致するリソースを確認した後、*IsDryRun* パラメータを False に設定して、一致するリソースのオブジェクトを古いホストから新しいホストに再リンクする必要があります。

- AutoMigrateManuallyAddedResources* パラメータはデフォルトで True に設定されており、手動で追加されたリソースが古いホストから新しいホストに自動的にコピーされます。

AutoMigrateManuallyAddedResources パラメータは、Oracle および SAP HANA リソースにのみ適用されます。

- 古いホストと新しいホストのインスタンス名が異なる場合は、*SQLInstanceMapping* パラメータを使用する必要があります。デフォルトのインスタンスの場合は、インスタンス名として *default_instance* を使用します。

機器更改は次のSnapCenterプラグインでサポートされています。

- SnapCenter Plug-in for Microsoft SQL Server
 - SQLデータベースがインスタンス レベルで保護されていて、ホストの機器更改の一環として一部のリソースのみが新しいホストに移動されると、既存のインスタンス レベルの保護がリソース グループ保護に変換され、両方のホストのインスタンスがリソース グループに追加されます。
 - SQLホスト（仮にhost1とする）が別のホスト（仮にhost2とする）のリソースのスケジューラまたは検証サーバとして使用されている場合は、host1で機器更改を実行している間、スケジュールまたは検証の詳細は移行されず、host1で引き続き実行されます。変更が必要な場合は、対応するホストで手動で変更する必要があります。
 - SQLフェイルオーバー クラスタ インスタンス（FCI） セットアップを使用している場合は、FCIクラスタに新しいノードを追加し、SnapCenterでプラグイン ホストを更新することで、機器更改を実行できます。
 - SQL可用性グループ（AG） セットアップを使用している場合は、機器更改は必要ありません。新しいノードをAGに追加し、SnapCenterでホストを更新できます。
- SnapCenter Plug-in for Windows
- SnapCenter Plug-in for Oracle Database

Oracle Real Application Cluster（RAC） セットアップを使用している場合は、RACクラスタに新しいノードを追加し、SnapCenterでプラグイン ホストを更新することで、機器更改を実行できます。

- SnapCenter Plug-in for SAP HANA Database

サポートされているユースケースは次のとおりです。

- あるホストから別のホストへのリソースの移行。
- 複数のホストからそれよりも少ない数（1つ以上）のホストへのリソースの移行。
- 1つのホストから複数のホストへのリソースの移行。

サポートされているシナリオは次のとおりです。

- 新しいホストの名前が古いホストと異なる
- 既存のホストの名前が変更された

開始する前に

このワークフローではSnapCenterリポジトリのデータが変更されるため、SnapCenterリポジトリをバックアップすることを推奨します。データに問題が発生した場合は、バックアップを使用してSnapCenterリポジトリを以前の状態に戻すことができます。

```
https://docs.netapp.com/us-en/snapcenter/admin/concept_manage_the_snapcenter_server_repository.html#back-up-the-snapcenter-repository["SnapCenterリポジトリのバックアップ"]。
```

手順

1. 新しいホストを導入し、アプリケーションをインストールします。

2. 古いホストのスケジュールを一時停止します。
3. 必要なリソースを古いホストから新しいホストに移動します。
 - a. 新しいホストで同じストレージから必要なデータベースを起動します。
 - ストレージが古いホストと同じドライブまたは同じマウントパスにマッピングされていることを確認します。ストレージが正しくマッピングされていないと、古いホストで作成されたバックアップをリストアに使用できません。



Windowsではデフォルトで、次に使用可能なドライブが自動的に割り当てられます。

- ストレージDRが有効になっている場合は、それぞれのストレージを新しいホストにマウントする必要があります。
- b. アプリケーションのバージョンに変更がある場合は、互換性を確認します。
 - c. Oracleプラグイン ホストの場合のみ、Oracleおよびそのグループ ユーザのUIDとGIDが古いホストのUIDとGIDと同じであることを確認します。

詳細については、以下を参照してください。

- ["How to migrate SQL database from old host to new host"](#)
- ["How to migrate Oracle database from old host to new host"](#)
- ["How to bring up SAP HANA database onto new host"](#)

4. 新しいホストをSnapCenterに追加します。
5. すべてのリソースが検出されたかどうかを確認します。
6. ホスト更新 API を実行します。`<snapcenter\_version>/techrefresh/host` またはコマンドレット: *Invoke-SmTechRefreshHost*。



ドライランはデフォルトで有効になっており、再リンクが必要な一致するリソースが特定されます。リソースを確認するには、API: `/jobs/{jobid}` またはコマンドレット *Get-SmJobSummaryReport* を実行します。

複数のホストからリソースを移行した場合は、すべてのホストに対してAPIまたはコマンドレットを実行する必要があります。新しいホストのドライブまたはマウントパスが古いホストと同じでない場合、次のリストア処理が失敗します。

- SQL In Placeリストアが失敗します。ただし、RTAL機能は利用できます。
- OracleデータベースとSAP HANAデータベースのリストアが失敗します。

複数のホストに移行する場合は、すべてのホストで手順1からの手順をすべて実行する必要があります。



同じホストでAPIまたはコマンドレットを複数回実行できます。再リンクは、新しいリソースが特定された場合にのみ実行されます。

7. (オプション) 古いホストをSnapCenterから削除します。

APIに関する情報については、Swaggerページにアクセスする必要があります。"[Swagger API Webページを使用してREST APIにアクセスする方法](#)"。

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

ストレージ システムの機器更改

ストレージの機器更改が行われると、データが新しいストレージに移行され、アプリケーション ホストが新しいストレージにマウントされます。SnapCenterのバックアップ ワークフローで新しいストレージが特定され、新しいストレージがSnapCenterに登録されている場合はSnapshotが作成されます。

ストレージ更改後に作成された新しいバックアップでは、リストア、マウント、およびクローニングを実行できます。ただし、バックアップには古いストレージの詳細が含まれているため、ストレージ更改前に作成されたバックアップに対してこれらの処理を実行すると失敗します。ストレージ機器更改のAPIまたはコマンドレットを実行して、SnapCenterの古いバックアップを新しいストレージの詳細で更新する必要があります。

機器更改は次のSnapCenterプラグインでサポートされています。

- SnapCenter Plug-in for Microsoft SQL Server
- SnapCenter Plug-in for Windows
- SnapCenter Plug-in for Oracle Database
- SnapCenter Plug-in for SAP HANA Database
- SnapCenter Plug-in for Microsoft Exchange Server

サポートされているユースケースは次のとおりです。

- プライマリ ストレージの更改

ストレージ機器更改では、プライマリ ストレージを新しいストレージに置き換えることができます。既存のセカンダリ ストレージをプライマリ ストレージに変換することはできません。

- セカンダリ ストレージの更改

プライマリ ストレージのバックアップの更新

ストレージの機器更改が完了したら、ストレージ機器更改のAPIまたはコマンドレットを実行して、SnapCenterの古いバックアップを新しいストレージの詳細で更新する必要があります。

開始する前に

このワークフローではSnapCenterリポジトリのデータが変更されるため、SnapCenterリポジトリをバックアップすることを推奨します。データに問題が発生した場合は、バックアップを使用してSnapCenterリポジトリを以前の状態に戻すことができます。

```
https://docs.netapp.com/us-en/snapcenter/admin/concept_manage_the_snapcenter_server_repository.html#back-up-the-snapcenter-repository["SnapCenterリポジトリのバックアップ"]。
```

手順

1. 古いストレージから新しいストレージにデータを移行します。

移行方法については、以下を参照してください。

- ["How to migrate the data to new storage"](#)
- ["ボリュームをコピーしてすべてのSnapshotコピーを保持するにはどうすればよいですか?"](#)

2. ホストをメンテナンス モードにします。
3. 新しいストレージをそれぞれのホストでマウントし、データベースを起動します。

新しいストレージは、以前と同じ方法でホストに接続する必要があります。たとえば、SANとして接続されていた場合は、SANとして接続する必要があります。

新しいストレージは、古いストレージと同じドライブまたはパスにマウントする必要があります。

4. すべてのリソースが動作していることを確認します。
5. SnapCenterで新しいストレージを追加します。

SnapCenterのクラスタ間でSVM名が一意であることを確認します。新しいストレージで同じSVM名を使用していて、ストレージ更改の実行前にSVMのすべてのボリュームを移行できる場合は、古いクラスタのSVMを削除したあとSnapCenterで古いクラスタを再検出してSVMをキャッシュから削除することを推奨します。

6. ホストを本番モードにします。
7. SnapCenterで、ストレージを移行するリソースのバックアップを作成します。SnapCenterで最新のストレージ フットプリントを特定するには、新しいバックアップが必要です。このバックアップは、既存の古いバックアップのメタデータを更新するために使用されます。



ホストに新しいLUNを接続すると、新しいシリアル番号が割り当てられます。Windowsファイルシステムの検出中、SnapCenterは一意のシリアル番号すべてを新しいリソースとして扱います。ストレージ機器更改時に、新しいストレージのLUNが同じドライブレターまたはパスでホストに接続される場合、SnapCenterでWindowsファイルシステムを検出すると、同じドライブレターまたはパスでマウントされていても、既存のリソースが削除済みとしてマークされ、新しいLUNが新しいリソースとして表示されます。リソースが削除済みとマークされていると、そのリソースはSnapCenterでストレージ機器更改の対象とはみなされません。そのため、古いリソースのバックアップはすべて失われます。Windowsファイルシステム リソースの場合、ストレージ更改を行う際は、ストレージの更改APIまたはコマンドレットを実行する前にリソースの検出を実行しないでください。

8. 次のいずれかのストレージ更新 API を実行します。`<snapcenter\_version>/techrefresh/primarystorage` またはコマンドレット: *Invoke-SmTechRefreshPrimaryStorage*。



レプリケーションが有効なポリシーがリソースに設定されている場合は、ストレージ更改後の最新のバックアップにセカンダリ ストレージの詳細が含まれます。

- a. SQLフェイルオーバー クラスタ インスタンス (FCI) セットアップを使用している場合、バックアップはクラスタ レベルで保持されます。ストレージ機器更改のために、クラスタ名を入力として指定する必要があります。
- b. SQL可用性グループ (AG) セットアップを使用している場合、バックアップはノード レベルで保持されます。ストレージ機器更改のために、ノード名を入力として指定する必要があります。
- c. Oracle Real Application Cluster (RAC) セットアップを使用している場合は、任意のノードでストレージ機器更改を実行できます。

IsDryRun 属性はデフォルトで True に設定されています。これで、ストレージが更改されているリソースが特定されます。API: '`<snapcenter_version>/jobs/{jobid}`' またはコマンドレット *Get-SmJobSummaryReport* を実行すると、リソースと変更されたストレージの詳細を表示できます。

9. ストレージの詳細を確認した後、*IsDryRun* 属性を False に設定し、ストレージ更新 API を実行します。
``<snapcenter_version>/techrefresh/primarystorage`` またはコマンドレット: *Invoke-SmTechRefreshPrimaryStorage*。

これで、古いバックアップのストレージの詳細が更新されます。

同じホストでAPIまたはコマンドレットを複数回実行できます。古いバックアップのストレージの詳細はストレージが更改された場合にのみ更新されます。



ONTAPでクローン階層を移行することはできません。移行対象のストレージのクローン メタデータがSnapCenter内にある場合、クローニングされたリソースは独立したリソースとしてマークされます。クローン メタデータのクローンは再帰的に削除されます。

10. (オプション) すべてのスナップショットが古いプライマリ ストレージから新しいプライマリ ストレージに移動されていない場合は、次の API を実行します。
``<snapcenter_version>/hosts/primarybackupsexistencecheck`` またはコマンドレット *Invoke-SmPrimaryBackupsExistenceCheck*。

これにより、新しいプライマリ ストレージでSnapshotの有無のチェックが行われ、対応するバックアップがSnapCenterでの処理に使用できないとマークされます。

セカンダリ ストレージのバックアップの更新

ストレージの機器更改が完了したら、ストレージ機器更改のAPIまたはコマンドレットを実行して、SnapCenterの古いバックアップを新しいストレージの詳細で更新する必要があります。

開始する前に

このワークフローではSnapCenterリポジトリのデータが変更されるため、SnapCenterリポジトリをバックアップすることを推奨します。データに問題が発生した場合は、バックアップを使用してSnapCenterリポジトリを以前の状態に戻すことができます。

```
https://docs.netapp.com/us-en/snapcenter/admin/concept_manage_the_snapcenter_server_repository.html#back-up-the-snapcenter-repository["SnapCenterリポジトリのバックアップ"]。
```

手順

1. 古いストレージから新しいストレージにデータを移行します。

移行方法については、以下を参照してください。

- ["How to migrate the data to new storage"](#)
- ["ボリュームをコピーしてすべてのSnapshotコピーを保持するにはどうすればよいですか？"](#)

2. プライマリ ストレージと新しいセカンダリ ストレージの間にSnapMirror関係を確立し、関係が正常な状態であることを確認します。
3. SnapCenterで、ストレージを移行するリソースのバックアップを作成します。

SnapCenterで最新のストレージ フットプリントを特定するには、新しいバックアップが必要です。このバックアップは、既存の古いバックアップのメタデータを更新するために使用されます。



この処理が完了するまで待つ必要があります。完了前に次の手順に進むと、SnapCenterで古いセカンダリSnapshotメタデータが完全に失われます。

4. ホスト内のすべてのリソースのバックアップを正常に作成したら、次のいずれかのセカンダリ ストレージ 更新 API を実行します。`<snapcenter\_version>/techrefresh/secondarystorage`またはコマンドレット: *Invoke-SmTechRefreshSecondaryStorage*。

これで、指定したホスト内の古いバックアップのセカンダリ ストレージの詳細が更新されます。

これをリソース レベルで実行する場合は、各リソースの **更新** をクリックして、セカンダリ ストレージのメタデータを更新します。

5. 古いバックアップが正常に更新されたら、プライマリとの古いセカンダリ ストレージ関係を解除できます。

SnapCenter Serverとプラグインのアンインストール

SnapCenterプラグイン パッケージのアンインストール

ホストを削除するための前提条件

SnapCenter GUI を使用して、ホストを削除したり、個々のプラグインまたはプラグイン パッケージをアンインストールしたりできます。また、SnapCenter Server ホストのコマンドライン インターフェイス (CLI) を使用するか、任意のホストでローカルに Windows の [プログラムのアンインストール] オプションを使用して、リモート ホスト上の個々のプラグインまたはプラグイン パッケージをアンインストールすることもできます。

SnapCenter Serverからホストを削除する前に、前提条件を満たしておく必要があります。

- 管理者としてログインする必要があります。
- ホストで検出ジョブが実行されていないことを確認する必要があります。
- ホストに関連付けられているすべてのオブジェクトを削除するためには、必要な権限を含むロールが割り当てられている必要があります。割り当てられていないと削除処理は失敗します。
- ホストをSnapCenterに追加した後に SSH キーが変更された場合は、フィンガープリントを確認する必要があります。
- SnapCenterホストがSnapCenterの新しいバージョンにアップグレードされているが、プラグイン ホストがまだプラグインの以前のバージョンを実行している場合は、フィンガープリントを確認する必要があります。

ロールベース アクセス制御を使用するホストを削除する場合の前提条件

- ホストの読み取りと削除、プラグインのインストールとアンインストール、およびオブジェクトの削除を行う権限を持つRBACロールを使用してログインしておく必要があります。

オブジェクトは、クローン、バックアップ、リソース グループ、ストレージ システムなどです。

- RBACロールにRBACユーザを追加しておく必要があります。
- 削除するホスト、プラグイン、クレデンシャル、リソース グループ、およびストレージ システム（クローンの場合）にRBACユーザを割り当てる必要があります。
- SnapCenterにRBACユーザとしてログインしておく必要があります。

クローン ライフサイクル処理で作成されたクローンを含むホストを削除する場合の前提条件

- SQLデータベースのクローン ライフサイクル管理を使用してクローニング ジョブを作成しておく必要があります。
- クローンの読み取りと削除、リソースの読み取りと削除、リソース グループの読み取りと削除、ストレージの読み取りと削除、プロビジョニングの読み取りと削除、マウント、アンマウント、プラグインのインストールとアンインストール、およびホストの読み取りと削除を行う権限を持つRBACロールを作成して

おく必要があります。

- RBACロールにRBACユーザを割り当てておく必要があります。
- ホスト、SnapCenter Plug-in for Microsoft SQL Server、クレデンシャル、クローン ライフサイクル リソース グループ、およびストレージ システムにRBACユーザを割り当てておく必要があります。
- SnapCenterにRBACユーザとしてログインしておく必要があります。

SnapCenter Plug-in for VMware vSphere のアンインストールについては、以下を参照してください。

["SnapCenter Plug-in for VMware vSphereの削除"](#)。

ホストを削除する

SnapCenter Serverでホストを削除すると、まずSnapCenterの[Resources]ページにそのホストに対して表示されているバックアップ、クローン、クローニング ジョブ、リソース グループ、およびリソースが削除され、次にホスト上のプラグイン パッケージがアンインストールされます。

タスク概要

- ホストを削除すると、そのホストに関連付けられているバックアップ、クローン、およびリソース グループも削除されます。
- リソース グループを削除すると、関連付けられているスケジュールもすべて削除されます。
- リソース グループを他のホストと共有しているホストを削除すると、リソース グループも削除されます。
- 廃止されたプラグイン ホストまたは到達できないプラグイン ホストを削除するには、*Remove-SmHost* コマンドレットを使用する必要があります。

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、["SnapCenterソフトウェア コマンドレット リファレンス ガイド"](#)

- ホストの削除にかかる時間は、バックアップの数と保持設定によって異なります。これは、各コントローラからSnapshotが削除され、メタデータが消去されるためです。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. *ホスト*ページで、*管理対象ホスト*をクリックします。
3. 削除するホストを選択し、[削除] をクリックします。
4. Oracle RAC クラスタの場合、クラスタ内のすべてのホストからSnapCenter softwareを削除するには、[クラスタのすべてのホストを含める] を選択します。

クラスタのノードを1つずつ削除することもできます。

5. [OK]をクリックします。



クラスタでホスト プラグインをアンインストールして再インストールしても、クラスタ リソースは自動的に検出されません。クラスター ホスト名を選択し、[リソースの更新] をクリックして、クラスター リソースを自動的に検出します。

SnapCenter GUIを使用したプラグインのアンインストール

個々のプラグインまたはプラグイン パッケージが不要になったと判断したら、SnapCenterインターフェイスを使用してアンインストールできます。

開始する前に

- アンインストールするプラグイン パッケージのリソース グループを削除しておく必要があります。
- アンインストールするプラグイン パッケージのリソース グループに関連付けられているポリシーを解除しておく必要があります。

タスク概要

プラグインは個別にアンインストールできます。たとえば、ホストのリソースが不足している場合に、SnapCenter Plug-in for Microsoft SQL Serverをアンインストールして、もっと余裕のあるホストに移動するというケースがあり得ます。プラグイン パッケージ全体をアンインストールすることもできます。たとえば、SnapCenter Plug-in for Oracle DatabaseとSnapCenter Plug-in for UNIXが含まれているSnapCenter Plug-ins Package for Linuxをアンインストールする必要がある場合があります。

- ホストを削除するとすべてのプラグインがアンインストールされる。

SnapCenterからホストを削除すると、SnapCenterはホストを削除する前にホスト上のすべてのプラグイン パッケージをアンインストールします。

- SnapCenter GUIでは一度に複数のホストからプラグインを削除できない。

SnapCenter GUIを使用する場合、プラグインをアンインストールできるホストは一度に1つです。ただし、複数のアンインストール処理を同時に実行できます。

Uninstall-SmHostPackage コマンドレットと必要なパラメータを使用して、複数のホストからプラグインをアンインストールすることもできます。コマンドレットで使用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。



SnapCenter ServerがインストールされているホストからSnapCenter Plug-ins Package for Windowsをアンインストールすると、インストールされているSnapCenter Serverが破損します。SnapCenter Serverが確実に不要になった場合を除き、SnapCenter Plug-ins Package for Windowsをアンインストールしないでください。

手順

1. 左側のナビゲーション ペインで、[ホスト] をクリックします。
2. [ホスト] ページで、[管理対象ホスト] をクリックします。
3. [Managed Hosts] ページで、プラグインまたはプラグイン パッケージをアンインストールするホストを選択します。
4. 削除したいプラグインの横にある [削除] > [送信] をクリックします。

終了後の操作

そのホストにプラグインを再インストールする場合は、5分間待ってください。この間にSnapCenter GUIで管理対象ホストのステータスが更新されます。プラグインをすぐに再インストールすると、インストールに失敗します。

Linux 用のSnapCenterプラグイン パッケージをアンインストールする場合、アンインストール固有のログ ファイルは `/custom_location/snapcenter/log` にあります。

PowerShellコマンドレットを使用したWindowsプラグインのアンインストール

SnapCenter Server ホストのコマンドライン インターフェイスで *Uninstall-SmHostPackage* コマンドレットを使用して、個々のプラグインをアンインストールしたり、1 つ以上のホストからプラグイン パッケージをアンインストールしたりできます。

プラグインをアンインストールする各ホストに対するローカルの管理者権限を持つドメイン ユーザとして、SnapCenterにログインしている必要があります。

手順

1. PowerShellを起動します。
2. SnapCenter Server ホストで、*Open-SMConnection -SMSbaseUrl https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME* コマンドを入力し、資格情報を入力します。
3. *Uninstall-SmHostPackage* コマンドレットと必要なパラメータを使用して、Windows プラグインをアンインストールします。

コマンドレットで利用できるパラメータとその説明に関する情報は、*Get-Help command_name* を実行すると取得できます。あるいは、"[SnapCenterソフトウェア コマンドレット リファレンス ガイド](#)"。

ホストでのプラグインのローカル アンインストール

SnapCenter Serverからホストに到達できない場合は、ホスト上でローカルにSnapCenterプラグインをアンインストールできます。

タスク概要

個々のプラグインまたはプラグイン パッケージをアンインストールするためのベストプラクティスは、SnapCenter GUIを使用するか、SnapCenter Serverホストのコマンドライン インターフェイスで*Uninstall-SmHostPackage*コマンドレットを使用することです。これらの手順を使用すると、SnapCenter Serverは変更を反映して最新の状態に保たれます。

ただしまれに、プラグインをローカルにアンインストールする必要がある場合があります。たとえば、SnapCenter Serverから実行したアンインストール ジョブが失敗した場合や、SnapCenter Serverのアンインストール後にプラグインだけがホストに残った場合などです。



ホスト上でローカルにプラグイン パッケージをアンインストールしても、スケジュールされたジョブやバックアップ メタデータなど、ホストに関連付けられているデータは削除されません。



SnapCenter Plug-ins Package for Windowsをコントロール パネルでローカルにアンインストールしないでください。SnapCenter Plug-in for Microsoft Windowsを確実にアンインストールするためには、SnapCenter GUIを使用する必要があります。

手順

1. ホスト システムで、コントロール パネルに移動し、[プログラムのアンインストール] をクリックします。
2. プログラムの一覧で、アンインストールするSnapCenterプラグインまたはプラグイン パッケージを選択し、[アンインストール] をクリックします。

選択したパッケージ内のすべてのプラグインがアンインストールされます。

CLIを使用したPlug-ins Package for LinuxまたはPlug-ins Package for AIXのアンインストール

SnapCenter Plug-ins Package for LinuxとSnapCenter Plug-ins Package for AIXは、コマンドライン インターフェイスを使用してアンインストールできます。

開始する前に

- スケジュール済みジョブが削除されていることを確認します。
- 実行中のすべてのジョブが完了していることを確認します。

手順

アンインストールするには、`/custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall` を実行します。

WindowsホストでのSnapCenter Serverのアンインストール

SnapCenter Serverを使用してデータ保護ジョブを管理する必要がなくなった場合は、SnapCenter Serverホストで[Control Panel]の[Programs and Features]を使用してSnapCenter Serverをアンインストールできます。SnapCenter Serverをアンインストールすると、そのコンポーネントがすべて削除されます。

開始する前に

- SnapCenter Serverがインストールされているドライブに2GB以上の空きスペースがあることを確認してください。
- SnapCenter Serverがインストールされているドメインが削除されていないことを確認してください。

SnapCenter Serverがインストールされているドメインを削除してからアンインストールを実行しようとすると、処理が失敗します。

- リポジトリ データベースもクリーンアップおよびアンインストールされるため、リポジトリ データベースをバックアップしておく必要があります。

手順

1. SnapCenter Serverホストで、[Control Panel]に移動します。
2. カテゴリ ビューになっていることを確認してください。
3. [プログラム] の下で、[プログラムのアンインストール] をクリックします。

[Programs and Features]ウィンドウが開きます。

4. NetApp SnapCenter Server を選択し、[アンインストール] をクリックします。

SnapCenter 4.2以降では、SnapCenter Serverをアンインストールすると、MySQL Serverリポジトリ データベースを含むすべてのコンポーネントがアンインストールされます。

- NLBクラスタからNLBノードを削除した場合、SnapCenter Serverホストを再起動する必要があります。ホストを再起動しないと、SnapCenter Serverを再インストールしようとしたときに失敗する可能性があります。
- .NET Frameworkはアンインストール時に削除されないため、手動でアンインストールする必要があります。

LinuxホストでのSnapCenter Serverのアンインストール

SnapCenter Serverを使用してデータ保護ジョブを管理する必要がなくなった場合は、SnapCenter Serverをアンインストールできます。SnapCenter Serverをアンインストールすると、そのコンポーネントがすべて削除されます。

手順

1. いずれかの操作を実行して、SnapCenter Serverをアンインストールします。

実行する処理	操作
非対話型アンインストール	<pre>\$ sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall -i silent -DCONFIRM=1</pre> 例：sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall
対話型アンインストール	<pre>\$ sudo <USER_INSTALL_DIR>/NetApp/snapcenter/SnapManagerWeb/installation/uninstall</pre> アンインストールを確認するためには、確認入力に0以外の値を入力します。

REST APIを使用したSnapCenterの自動化

REST APIを使用したSnapCenterの自動化

REST API を使用して、いくつかのSnapCenter管理操作を実行できます。REST API はSwagger Webページから利用できます。

`https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/` にある Swagger Web ページにアクセスして、REST API ドキュメントを表示したり、API 呼び出しを手動で発行したりできます。

REST APIをサポートするプラグインは次のとおりです。

- Plug-in for Microsoft SQL Server
- Plug-in for SAP HANA Database
- Plug-in for Oracle Database

SnapCenter Plug-in for VMware vSphereの詳細については、以下を参照してください。 ["SnapCenter Plug-in for VMware vSphere"](#)

SnapCenter REST APIへネイティブにアクセスする方法

SnapCenter REST APIには、RESTクライアントをサポートする任意のプログラミング言語を使用して直接アクセスできます。よく使われる言語には、Python、PowerShell、Javaなどがあります。

基盤としてのREST Webサービス

Representational State Transfer (REST) は、分散Webアプリケーションの作成に使用される形式です。WebサービスAPIの設計においては、これによってサーバベースのリソースの公開とその状態の管理に関する一連のテクノロジーとベストプラクティスが確立されます。主流のプロトコルと標準が使用されており、SnapCenterを管理するための柔軟な基盤が提供されます。

リソースと状態の表示

リソースはWebベース システムの基本コンポーネントです。REST Webサービス アプリケーションを作成する場合、設計の早い段階で次の作業を行います。

システムまたはサーバベースのリソースの識別

すべてのシステムは、リソースを使用し、管理します。リソースには、ファイル、ビジネス トランザクション、プロセス、管理エンティティなどがあります。REST Webサービスに基づいてアプリケーションを設計する際に行う最初の作業の1つは、リソースを識別することです。

リソースの状態の定義および関連する状態処理

リソースは必ず複数ある状態のいずれかに該当します。状態は明確に定義する必要があり、状態の変化に作用する操作も明確に定義する必要があります。

URIエンドポイント

すべてのRESTリソースは、明確に定義されたアドレス指定方式を使用して定義、提供される必要があります。リソースが置かれているエンドポイントは、Uniform Resource Identifier（URI）で識別されます。

URIは、ネットワークの各リソースに一意の名前を作成するための一般的なフレームワークです。Uniform Resource Locator（URL）は、リソースを識別してアクセスするためにWebサービスで使用されるURIの一種です。リソースは、通常、ファイルディレクトリに似た階層構造で公開されます。

HTTPメッセージ

Hypertext Transfer Protocol（HTTP）は、Webサービスのクライアントとサーバがリソースに関する要求と応答のメッセージを交換する際に使用するプロトコルです。

Webサービスアプリケーションの設計の一環として、リソースおよび対応する状態管理アクションにHTTPメソッドがマッピングされます。HTTPはステートレスです。したがって、関連する一連の要求と応答を1つのトランザクションの一部として関連付けるには、要求と応答のデータフローで伝送されるHTTPヘッダーに追加情報を含める必要があります。

JSONの形式

Webサービスのクライアントとサーバの間で情報を構造化したり転送したりする方法は複数ありますが、最も広く使用されているのはJavaScript Object Notation（JSON）です。

JSONは、単純なデータ構造をプレーンテキストで表現するための業界標準であり、リソースについての状態情報の転送に使用されます。SnapCenter REST APIでは、JSONを使用して、各HTTP要求と応答の本文で伝送されるデータをフォーマットします。

基本的な動作の特性

RESTで共通のテクノロジーとベストプラクティスは確立されますが、各APIの詳細は設計内容に応じて異なる場合があります。

要求と応答のAPIトランザクション

すべてのREST API呼び出しは、SnapCenter ServerシステムへのHTTP要求として実行され、クライアントへの関連する応答が生成されます。この要求と応答のペアでAPIトランザクションが構成されます。

APIを使用する前に、要求の制御に使用できる入力変数と応答出力の内容を理解しておく必要があります。

CRUD操作のサポート

SnapCenter REST APIで利用できる各リソースへのアクセスはCRUDモデルに基づきます。

- 作成

- 読み取り
- 更新
- 削除

リソースによっては、一部の操作のみがサポートされるものもあります。

オブジェクトID

リソース インスタンスまたはオブジェクトには、作成時に一意の識別子がそれぞれ割り当てられます。ほとんどの場合、識別子は128ビットのUUIDです。これらの識別子は、特定のSnapCenter Server内でグローバルに一意です。

新しいオブジェクト インスタンスを作成するAPI呼び出しを発行すると、関連付けられたIDを含むURLがHTTP応答のlocationヘッダーに記載されて呼び出し元に返されます。リソース インスタンスを以降の呼び出しで参照する際は、この識別子を抽出して使用できます。



オブジェクト識別子の内容と内部構造は変更になることがあります。識別子を使用するのは、該当するAPI呼び出しで関連付けられているオブジェクトを参照するために必要な場合だけにしてください。

オブジェクトのインスタンスとコレクション

リソース パスとHTTPメソッドに応じて、API呼び出しを特定のオブジェクト インスタンスまたはオブジェクトのコレクションに適用できます。

同期操作と非同期操作

SnapCenterは、クライアントから受信したHTTP要求を同期または非同期で実行します。

同期処理

SnapCenterは要求をすぐに実行し、HTTPステータス コード200または201（成功した場合）を返します。

GETメソッドを使用する要求はすべて、常に同期的に実行されます。また、POSTを使用する要求は、完了までに2秒かからないと予想される場合は同期的に実行するように設計されています。

非同期処理

非同期要求が有効な場合、SnapCenterは、要求を処理するバックグラウンド タスクとそのタスクのアンカーを設定するジョブ オブジェクトを作成します。HTTPステータス コード202がジョブ オブジェクトとともに呼び出し元に返されます。成功したかどうかを判断するには、ジョブの状態を取得する必要があります。

POSTとDELETEの各メソッドを使用する要求は、完了までに2秒以上かかると予想される場合は非同期で実行するように設計されています。

セキュリティ

REST APIのセキュリティは、主にSnapCenterで利用可能な既存のセキュリティ機能に基づいています。APIで使用されるセキュリティは次のとおりです。

Transport Layer Security

SnapCenter Serverとクライアントの間でネットワークを介して送信されるトラフィックは、SnapCenter構成の設定に基づいて、通常はTLSを使用してすべて暗号化されます。

HTTP認証

HTTPレベルでは、APIトランザクションにベーシック認証が使用されます。base64文字列のユーザ名とパスワードを含むHTTPヘッダーが各要求に追加されます。

API要求を制御する入力変数

API呼び出しの処理方法は、HTTP要求で設定されたパラメータと変数を使用して制御できます。

HTTPメソッド

次の表に、SnapCenter REST APIでサポートされるHTTPメソッドを示します。



RESTエンドポイントのそれぞれですべてのHTTPメソッドを使用できるわけではありません。

HTTPメソッド	説明
GET	リソース インスタンスまたはコレクションのオブジェクトのプロパティを取得します。
POST	指定された入力に基づいて新しいリソース インスタンスを作成します。
DELETE	既存のリソース インスタンスを削除します。
PUT	既存のリソース インスタンスを変更します。

要求ヘッダー

HTTP要求には複数のヘッダーを含める必要があります。

Content-type

リクエスト本文に JSON が含まれている場合、このヘッダーは *application/json* に設定する必要があります。

受け入れる

このヘッダーは *application/json* に設定する必要があります。

承認

base64文字列としてエンコードされたユーザ名とパスワードを使用するベーシック認証を設定する必要があります。

リクエスト本文

要求の本文の内容は、それぞれの呼び出しに応じて異なります。HTTP要求の本文は、次のいずれかで構成されます。

- JSONオブジェクトと入力変数
- 空の

オブジェクトのフィルタ

GETを使用するAPI呼び出しを発行する際、返されるオブジェクトを任意の属性に基づいて制限またはフィルタできます。たとえば、一致する完全な値を指定できます。

<field>=<query value>

完全一致に加えて、他の演算子を使用して、特定の範囲の値の一連のオブジェクトを返すことができます。次の表に、SnapCenter REST APIでサポートされるフィルタ演算子を示します。

オペレーター	説明
=	等しい
<	小なり
>	より大きい
≤	以下
≥	より大きいか等しい
UPDATE	または
!	等しくない
*	すべてに一致するワイルドカード

クエリの一部として **null** キーワードまたはその否定 **!null** を使用することで、特定のフィールドが設定されているかどうかに基づいてオブジェクトのコレクションを返すこともできます。



通常、設定されていないフィールドはクエリの照合から除外されます。

特定のオブジェクト フィールドの要求

デフォルトでは、GETを使用してAPI呼び出しを実行すると、1つまたは複数のオブジェクトを一意に識別する属性のみが返されます。この最小のフィールド セットは各オブジェクトのキーとして機能し、オブジェクト タイプによって異なります。追加のオブジェクトプロパティを選択するには、`fields` クエリパラメータを次の方法で指定します。

共通または標準のフィールド

最もよく使用されるオブジェクト フィールドを取得するには、**fields=*** を指定します。通常、これらのフィールドはローカル サーバ メモリに保持されているか、ほとんど処理を必要とせずにアクセスできます。これらのプロパティは、URLパス キー (UUID) を指定してGETを使用した場合にオブジェクトに対して返されるプロパティと同じです。

すべてのフィールド

fields=** を指定すると、アクセスするために追加のサーバー処理が必要なものも含め、すべてのオブジェクト フィールドが取得されます。

カスタム フィールド選択

必要なフィールドを正確に指定するには、**fields=<field_name>** を使用します。複数のフィールドを要求する場合は、各値の間にスペースを入れずにカンマで区切る必要があります。



ベストプラクティスとして、必要なフィールドを常に個別に指定することを推奨します。一連の共通のフィールドやすべてのフィールドを取得するのは、必要な場合だけにしてください。どのフィールドが共通として分類され、*fields=** を使用して返されるかは、NetAppによって内部パフォーマンス分析に基づいて決定されます。フィールドの分類は、今後のリリースで変更される可能性があります。

出力セット内のオブジェクトのソート

リソース コレクション内のレコードは、オブジェクトで定義されたデフォルトの順序で返されます。順序を変更するには、`order_by` フィールド名と並べ替え方向を指定したクエリ パラメータは次のとおりです。

```
order_by=<field name> asc|desc
```

たとえば、次のように指定すると、`type` フィールドで降順にソートしてから、`id` で昇順にソートできます。

```
order_by=type desc, id asc
```

- ソートするフィールドを指定してソート順序を指定しなかった場合、値は昇順でソートされます。
- 複数のパラメータを指定する場合は、各フィールドをカンマで区切る必要があります。

オブジェクトのコレクションを取得するときのページ付け

GETを使用するAPI呼び出しを発行して同じタイプのオブジェクトのコレクションにアクセスする場合、SnapCenterでは2つの制約に基づいて可能な限り多くのオブジェクトを返します。これらの各制約は、要求に対する追加のクエリ パラメータを使用して制御できます。それぞれのGET要求に対する最初の制約に達した時点で要求が終了され、結果として返されるレコードの数が制限されます。



すべてのオブジェクトについての処理が完了する前に要求が終了した場合、次のレコードのバッチを取得するために必要なリンクが応答に含まれます。

オブジェクト数の制限

デフォルトでは、SnapCenter はGET リクエストに対して最大 10,000 個のオブジェクトを返します。この制限は、*max_records* クエリ パラメータを使用して変更できます。例えば：

```
max_records=20
```

実際に返されるオブジェクトの数は、関連する時間の制約やシステム内のオブジェクトの総数に基づいて、有効な最大数よりも少なくなることがあります。

オブジェクトを取得する時間の制限

デフォルトでは、SnapCenterはGET要求に許可された時間の範囲内でできるだけ多くのオブジェクトを返します。デフォルトのタイムアウトは15秒です。この制限は、`return_timeout` クエリ パラメータを使用して変更できます。例えば：

```
return_timeout=5
```

実際に返されるオブジェクトの数は、関連するオブジェクト数の制約やシステム内のオブジェクトの総数に基づいて、有効な最大数よりも少なくなることがあります。

結果セットの絞り込み

必要に応じて、これらの2つのパラメータを追加のクエリ パラメータと組み合わせて、結果セットを絞り込むことができます。たとえば、次の例では、指定した時間のあとに生成されたEMSイベントを最大10件まで返します。

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

複数の要求を発行してオブジェクトをページングすることができます。以降のAPI呼び出しでは、前回の結果セットの最後のイベントに基づいて新しい時間の値を使用する必要があります。

サイズのプロパティ

一部のAPI呼び出しおよびクエリ パラメータでは、入力値として数値が使用されます。バイト単位で整数を指定する代わりに、必要に応じて次の表に示すサフィックスを使用することができます。

サフィックス	説明
KB	KB：キロバイト（1,024バイト）またはキビバイト
MB	MB：メガバイト（KB x 1,024バイト）またはメビバイト
GB	GB：ギガバイト（MB x 1,024バイト）またはギビバイト
TB	TB：テラバイト（GB x 1,024バイト）またはテビバイト
PB	PB：ペタバイト（TB x 1,024バイト）またはペビバイト

API応答の解釈

各API要求でクライアントへの応答が生成されます。要求が成功したかどうかを確認したり、必要に応じて追加データを取得したりするには、応答を調べる必要があります。

HTTPステータス コード

SnapCenter REST APIで使用されるHTTPステータス コードを次に示します。

コード	説明
200	OK 新しいオブジェクトを作成しない呼び出しが成功したことを示します。
201	作成されました オブジェクトが正常に作成されました。応答のlocationヘッダーにオブジェクトの一意の識別子が含まれます。
202	承認済み 要求を実行するためにバックグラウンド ジョブが開始されましたが、まだ完了していません。
400	不正なリクエスト リクエストの入力が認識されないか不適切です。
401	不正なユーザー認証に失敗しました。
403	承認 (RBAC) エラーのため、禁止アクセスは拒否されました。
404	見つかりません。リクエストで参照されたリソースが存在しません。
405	メソッドは許可されていません。リクエスト内の HTTP メソッドはリソースではサポートされていません。
409	競合 別のオブジェクトを最初に作成する必要があるか、要求されたオブジェクトがすでに存在するため、オブジェクトの作成に失敗しました。
500	内部エラー サーバーで一般的な内部エラーが発生しました。

応答ヘッダー

SnapCenterによって生成されるHTTP応答には、いくつかのヘッダーが含まれています。

Location

オブジェクトが作成されたときに、オブジェクトに割り当てられた一意の識別子を含む、新しいオブジェクトへの完全なURLが含まれます。

Content-type

これは通常 application/json。

応答の本文

API要求の結果として返される応答の本文の内容は、オブジェクト、処理タイプ、および要求の成否によって異なります。応答は常にJSON形式になります。

単一のオブジェクト

単一のオブジェクトを要求に基づいて一連のフィールドとともに返すことができます。たとえば、GETで一意の識別子を使用して、クラスタの選択したプロパティを取得できます。

複数のオブジェクト

リソース コレクションから複数のオブジェクトを返すことができます。いずれの場合も、一貫した形式が使用されます。`num\_records`レコード数と、オブジェクトインスタンスの配列を含むレコード数を示します。たとえば、特定のクラスタで定義されているノードを取得できます。

ジョブ オブジェクト

API呼び出しが非同期で処理されると、バックグラウンド タスクのアンカーを設定するジョブ オブジェクトが返されます。たとえば、クラスタ構成の更新に使用されるPATCH要求は非同期で処理され、ジョブ オブジェクトが返されます。

エラー オブジェクト

エラーが発生した場合は、常にエラー オブジェクトが返されます。たとえば、クラスタに定義されていないフィールドを変更しようとするエラーが返されます。

空の

場合によっては、データが返されず、応答の本文に空のJSONオブジェクトが含まれることがあります。

エラー

エラーが発生した場合は、応答の本文でエラー オブジェクトが返されます。

フォーマット

エラー オブジェクトの形式は次のとおりです。

```
"error": {
  "message": "<string>",
  "code": <integer>[,
  "target": "<string>"]
}
```

codeの値で一般的なエラーの種類やカテゴリを特定し、messageで具体的なエラーの内容を確認できます。特定可能な場合は、エラーに関連するユーザ入力targetフィールドに含まれます。

一般的なエラー コード

次の表に一般的なエラー コードを示します。特定のAPI呼び出しについては、追加のエラー コードが含まれる場合があります。

コード	説明
409	同じ識別子のオブジェクトがすでに存在します。
400	フィールドの値が無効であるか、値が指定されていないか、不要なフィールドが指定されています。
400	この操作はサポートされていません。

コード	説明
405	指定した識別子を持つオブジェクトが見つかりません。
403	要求を実行する権限が拒否されました。
409	リソースが使用中です。

SnapCenter ServerとプラグインでサポートされているREST API

SnapCenter REST APIで使えるリソースは、SnapCenter APIドキュメント ページに表示されるカテゴリ別に分類されています。ここでは、各リソースの簡単な説明と基本リソースパスを示し、使用に際しての追加の考慮事項がある場合はその情報も示します。

認証

このAPIを使用すると、SnapCenter Serverにログインできます。このAPIは、以降の要求を認証するために使用されるユーザ認証トークンを返します。

ドメイン

APIを使用して、次のようなさまざまな処理を実行できます。

- SnapCenterのすべてのドメインを取得する
- 特定のドメインの詳細を取得する
- ドメインの登録や登録解除を行う
- ドメインを変更する

ジョブ

APIを使用して、次のようなさまざまな処理を実行できます。

- SnapCenterのすべてのジョブを取得する
- ジョブのステータスを取得する
- ジョブをキャンセルまたは停止する

設定

APIを使用して、次のようなさまざまな処理を実行できます。

- クレデンシャルを登録、変更、削除する
- SnapCenter Serverに登録されているクレデンシャル情報を表示する
- 通知を設定する

- 現在Eメール通知を送信するように設定されているSMTPサーバに関する情報を取得し、SMTPサーバ名、受信者名、送信者名を表示する
- SnapCenter Serverへのログインの多要素認証（MFA）設定を表示する
- SnapCenter ServerへのログインのMFAの有効 / 無効の切り替えや設定を行う
- MFAのセットアップに必要な構成ファイルを作成する

ホスト

APIを使用して、次のようなさまざまな処理を実行できます。

- すべてのSnapCenterホストを照会する
- SnapCenterから1つ以上のホストを削除する
- 名前を指定してホストを取得する
- ホスト上のすべてのリソースを取得する
- リソースIDを使用してリソースを取得する
- プラグイン設定の詳細を取得する
- プラグイン ホストを設定する
- Microsoft SQL Serverホスト用プラグインのすべてのリソースを取得する
- Oracleデータベース ホスト用プラグインのすべてのリソースを取得する
- カスタム アプリケーション ホスト用プラグインのすべてのリソースを取得する
- SAP HANAホスト用プラグインのすべてのリソースを取得する
- インストールされているプラグインを取得する
- 既存のホストにプラグインをインストールする
- ホスト パッケージをアップグレードする
- 既存のホストからプラグインを削除する
- ホストにプラグインを追加する
- ホストを追加または変更する
- Linuxホストのシグネチャを取得する
- Linuxホストのシグネチャを登録する
- ホストをメンテナンス モードまたは本番モードにする
- ホストのプラグイン サービスを開始または再起動する
- ホストの名前を変更する

リソース

APIを使用して、次のようなさまざまな処理を実行できます。

- すべてのリソースを取得する

- リソースIDを使用してリソースを取得する
- Microsoft SQL Serverホスト用プラグインのすべてのリソースを取得する
- Oracleデータベース ホスト用プラグインのすべてのリソースを取得する
- カスタム アプリケーション ホスト用プラグインのすべてのリソースを取得する
- SAP HANAホスト用プラグインのすべてのリソースを取得する
- キーを使用してMicrosoft SQL Serverのリソースを取得する
- キーを使用してカスタム リソースを取得する
- カスタム アプリケーション ホスト用プラグインのリソースを変更する
- キーを使用してカスタム アプリケーション ホスト用プラグインのリソースを削除する
- キーを使用してSAP HANAのリソースを取得する
- SAP HANAホスト用プラグインのリソースを変更する
- キーを使用してSAP HANAホスト用プラグインのリソースを削除する
- キーを使用してOracleのリソースを取得する
- Oracleアプリケーション ボリュームのリソースを作成する
- Oracleアプリケーション ボリュームのリソースを変更する
- キーを使用してOracleアプリケーション ボリュームのリソースを削除する
- Oracleのリソースに関するセカンダリの詳細を取得する
- Plug-in for Microsoft SQL Serverを使用してMicrosoft SQL Serverのリソースをバックアップする
- Plug-in for Oracle Databaseを使用してOracleのリソースをバックアップする
- カスタム アプリケーション用プラグインを使用してカスタム リソースをバックアップする
- SAP HANAデータベースを設定する
- Oracleデータベースを設定する
- SQLデータベースのバックアップをリストアする
- Oracleデータベースのバックアップをリストアする
- カスタム アプリケーションのバックアップをリストアする
- SAP HANAのリソースを作成する
- カスタム アプリケーション用プラグインを使用してカスタム リソースを保護する
- Plug-in for Microsoft SQL Serverを使用してMicrosoft SQL Serverのリソースを保護する
- 保護対象のMicrosoft SQL Serverのリソースを変更する
- Microsoft SQL Serverのリソースの保護を解除する
- Plug-in for Oracle Databaseを使用してOracleのリソースを保護する
- 保護対象のOracleリソースを変更する
- Oracleのリソースの保護を解除する
- カスタム アプリケーション用プラグインを使用してバックアップからリソースをクローニングする

- Plug-in for Oracle Databaseを使用してバックアップからOracleアプリケーション ボリュームをクローニングする
- Plug-in for Microsoft SQL Serverを使用してバックアップからMicrosoft SQL Serverのリソースをクローニングする
- Microsoft SQL Serverのリソースのクローン ライフサイクルを作成する
- Microsoft SQL Serverのリソースのクローン ライフサイクルを変更する
- Microsoft SQL Serverのリソースのクローン ライフサイクルを削除する
- 既存のMicrosoft SQL Serverデータベースをローカル ディスクからNetApp LUNに移動する
- Oracleデータベースのクローン仕様ファイルを作成する
- Oracleのリソースのクローン更新ジョブをオンデマンドで開始する
- クローン仕様ファイルを使用してバックアップからOracleのリソースを作成する
- データベースをセカンダリ レプリカにリストアし、データベースを可用性グループに再参加させる
- Oracleアプリケーション ボリュームのリソースを作成する

バックアップ

APIを使用して、次のようなさまざまな処理を実行できます。

- バックアップの名前、タイプ、プラグイン、リソース、日付を指定してバックアップの詳細を取得する
- すべてのバックアップを取得する
- バックアップの詳細を取得する
- バックアップの名前変更または削除を行う
- Oracleのバックアップをマウントする
- Oracleのバックアップをアンマウントする
- Oracleのバックアップをカタログに登録する
- Oracleのバックアップをカタログから削除する
- ポイントインタイム リカバリを実行するためにマウントする必要があるバックアップをすべて取得する

クローン

APIを使用して、次のようなさまざまな処理を実行できます。

- Oracleデータベースのクローン仕様ファイルを作成、表示、変更、削除する
- Oracleデータベースのクローン階層を表示する
- クローンの詳細を取得する
- すべてのクローンを取得する
- クローンを削除する
- IDを指定してクローンの詳細を取得する
- Oracleのリソースのクローン更新ジョブをオンデマンドで開始する

- クローン仕様ファイルを使用してバックアップからOracleのリソースをクローニングする

クローン スプリット

APIを使用して、次のようなさまざまな処理を実行できます。

- クローン リソースのクローン スプリット処理を概算する
- クローン スプリット処理のステータスを取得する
- クローン スプリット処理を開始または停止する

リソース グループ

APIを使用して、次のようなさまざまな処理を実行できます。

- すべてのリソース グループの詳細を取得する
- 名前を指定してリソース グループを取得する
- カスタム アプリケーション用プラグインのリソース グループを作成する
- Plug-in for Microsoft SQL Serverのリソース グループを作成する
- Plug-in for Oracle Databaseのリソース グループを作成する
- カスタム アプリケーション用プラグインのリソース グループを変更する
- Plug-in for Microsoft SQL Serverのリソース グループを変更する
- Plug-in for Oracle Databaseのリソース グループを変更する
- Plug-in for Microsoft SQL Serverのリソース グループのクローン ライフサイクルを作成、変更、削除する
- リソース グループをバックアップする
- リソース グループをメンテナンス モードまたは本番モードにする
- リソース グループを削除する

ポリシー

APIを使用して、次のようなさまざまな処理を実行できます。

- ポリシーの詳細を取得する
- 名前を指定してポリシーの詳細を取得する
- ポリシーを削除する
- 既存のポリシーのコピーを作成する
- カスタム アプリケーション用プラグインのポリシーを作成または変更する
- Plug-in for Microsoft SQL Serverのポリシーを作成または変更する
- Plug-in for Oracle Databaseのポリシーを作成または変更する
- Plug-in for SAP HANA Databaseのポリシーを作成または変更する

ストレージ

APIを使用して、次のようなさまざまな処理を実行できます。

- すべての共有を取得する
- 名前を指定して共有を取得する
- 共有を作成または削除する
- ストレージの詳細を取得する
- 名前を指定してストレージの詳細を取得する
- ストレージを作成、変更、削除する
- ストレージ クラスタ上のリソースを検出する
- ストレージ クラスタ上のリソースを取得する

共有

APIを使用して、次のようなさまざまな処理を実行できます。

- 共有の詳細を取得する
- すべての共有の詳細を取得する
- ストレージ上の共有を作成または削除する
- 名前を指定して共有を取得する

プラグイン

APIを使用して、次のようなさまざまな処理を実行できます。

- ホストのすべてのプラグインを一覧表示する
- キーを使用してMicrosoft SQL Serverのリソースを取得する
- キーを使用してカスタム リソースを変更する
- キーを使用してカスタム リソースを削除する
- キーを使用してSAP HANAのリソースを取得する
- キーを使用してSAP HANAのリソースを変更する
- キーを使用してSAP HANAのリソースを削除する
- キーを使用してOracleのリソースを取得する
- キーを使用してOracleアプリケーション ボリュームのリソースを変更する
- キーを使用してOracleアプリケーション ボリュームのリソースを削除する
- Plug-in for Microsoft SQL Serverとキーを使用してMicrosoft SQL Serverのリソースをバックアップする
- Plug-in for Oracle Databaseとキーを使用してOracleのリソースをバックアップする
- カスタム アプリケーション用のプラグインとキーを使用してカスタム アプリケーションのリソースをバックアップする

- キーを使用してSAP HANAデータベースを設定する
- キーを使用してOracleデータベースを設定する
- キーを使用してカスタム アプリケーションのバックアップをリストアする
- SAP HANAのリソースを作成する
- Oracleアプリケーション ボリュームのリソースを作成する
- カスタム アプリケーション用プラグインを使用してカスタム リソースを保護する
- Plug-in for Microsoft SQL Serverを使用してMicrosoft SQL Serverのリソースを保護する
- 保護対象のMicrosoft SQL Serverのリソースを変更する
- Microsoft SQL Serverのリソースの保護を解除する
- Plug-in for Oracle Databaseを使用してOracleのリソースを保護する
- 保護対象のOracleリソースを変更する
- Oracleのリソースの保護を解除する
- カスタム アプリケーション用プラグインを使用してバックアップからリソースをクローニングする
- Plug-in for Oracle Databaseを使用してバックアップからOracleアプリケーション ボリュームをクローニングする
- Plug-in for Microsoft SQL Serverを使用してバックアップからMicrosoft SQL Serverのリソースをクローニングする
- Microsoft SQL Serverのリソースのクローン ライフサイクルを作成する
- Microsoft SQL Serverのリソースのクローン ライフサイクルを変更する
- Microsoft SQL Serverのリソースのクローン ライフサイクルを削除する
- Oracleデータベースのクローン仕様ファイルを作成する
- Oracleリソースのクローン ライフサイクルをオンデマンドで開始する
- クローン仕様ファイルを使用してバックアップからOracleのリソースをクローニングする

レポート

APIを使用して、次のようなさまざまな処理を実行できます。

- 各プラグインのバックアップ、リストア、クローニング処理のレポートを取得する
- スケジュールを追加、実行、削除、変更する
- スケジュール済みレポートのデータを取得する

アラート

APIを使用して、次のようなさまざまな処理を実行できます。

- すべてのアラートを取得する
- IDを指定してアラートを取得する
- 複数のアラートを削除する、またはIDを指定してアラートを削除する

RBAC

APIを使用して、次のようなさまざまな処理を実行できます。

- ユーザ、グループ、ロールの詳細を取得する
- ユーザを追加または削除する
- ロールにユーザを割り当てる
- ロールへのユーザの割り当てを解除する
- ロールを作成、変更、削除する
- グループをロールに割り当てる
- ロールへのグループの割り当てを解除する
- グループを追加または削除する
- 既存のロールのコピーを作成する
- ユーザまたはグループへのリソースの割り当てや割り当ての解除を行う

構成

APIを使用して、次のようなさまざまな処理を実行できます。

- 構成設定を表示する
- 構成設定を変更する

証明書設定

APIを使用して、次のようなさまざまな処理を実行できます。

- SnapCenter Serverまたはプラグインホストの証明書ステータスを表示する
- SnapCenter Serverまたはプラグインホストの証明書設定を変更する

リポジトリ

APIを使用して、次のようなさまざまな処理を実行できます。

- リポジトリ バックアップを取得する
- リポジトリに関する設定情報を表示する
- SnapCenterリポジトリを保護、リストアする
- SnapCenterリポジトリの保護を解除する
- リポジトリを再構築したりフェイルオーバーしたりする

version

このAPIを使用すると、SnapCenterのバージョンを表示できます。

Swagger API WebページからREST APIにアクセスする方法

REST APIはSwagger Webページから利用できます。Swagger Webページにアクセスして、SnapCenter Server REST APIを表示したり、APIを手動で呼び出したりすることができます。REST APIを使用して、SnapCenter Serverの管理やデータ保護処理を行うことができます。

REST APIを実行するSnapCenter Serverの管理IPアドレスまたはドメイン名を確認しておく必要があります。

REST APIクライアントを実行するために特別な権限は必要ありません。すべてのユーザがSwagger Webページにアクセスできます。REST APIでアクセスするオブジェクトに対する権限は、REST APIへのログインに使用するトークンを生成したユーザに基づきます。

手順

1. ブラウザから、`https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/` の形式で Swagger Web ページにアクセスするための URL を入力します。



REST API URL に +、.、%、& の文字が含まれていないことを確認します。

2. **Swagger Explore** フィールドに、Swagger API ドキュメントが自動的に表示されない場合は、次のように入力します: `https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/Content/swagger/SnapCenter.yaml`
3. *探索*をクリックします。

APIリソース タイプ（カテゴリ）の一覧が表示されます。

4. APIリソース タイプをクリックすると、そのリソース タイプのAPIが表示されます。

SnapCenter REST APIの実行時に予期しない動作が発生した場合は、ログ ファイルで原因を特定して問題を解決することができます。モニター > ログ > ダウンロード をクリックすると、SnapCenterユーザー インターフェイスからログ ファイルをダウンロードできます。

REST APIの使用の開始

SnapCenter REST APIはすぐに使用を開始できます。APIにアクセスすると、稼働中の設定で複雑なワークフロー プロセスを使用する前にいくつかの情報を確認できます。

Hello world

システムで簡単なコマンドを実行して、SnapCenter REST APIの使用を開始し、使用できるかどうかを確認できます。

開始する前に

- システムでcURLユーティリティが使用可能なことの確認
- SnapCenter ServerのIPアドレスまたはホスト名
- SnapCenter REST APIにアクセスする権限を持つアカウントのユーザ名とパスワード



クレデンシャルに特殊文字が含まれている場合は、使用するシェルに基づいてCurlで受け入れられる形式で指定する必要があります。たとえば、各特殊文字の前にバックスラッシュを挿入したり、全体を囲んだりすることができます。`username:password`一重引用符で囲んだ文字列。

手順

コマンドライン インターフェイスで、次のコマンドを実行してプラグイン情報を取得します。

```
curl -X GET -u username:password -k  
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

例：

```
curl -X GET -u admin:password -k  
"'https://10.225.87.97/api/hosts?fields=IncludePluginInfo'"
```

法律上の表示

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

プライバシー ポリシー

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

オープンソース

通知ファイルには、NetAppソフトウェアで使用するサードパーティの著作権およびライセンスに関する情報が提供されます。

["SnapCenter 6.1 に関するお知らせ"](#)

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。