Documentação do SnapCenter software

SnapCenter software

NetApp
September 29, 2025

Índice

Documentação do SnapCenter software . . . 1
Notas de lançamento . . . 2
Notas de lançamento . . . 2
Caminhos de atualização suportados para SnapCenter . . . 2
Começar . . . 3
Saiba mais sobre o SnapCenter software . . . 3
Visão geral do SnapCenter . . . 3
Recursos de segurança no SnapCenter . . . 7
Controle de acesso baseado em função no SnapCenter . . . 9
Recuperação de desastres no SnapCenter . . . 14
Licenças exigidas pelo SnapCenter . . . 15
Sincronização ativa do SnapMirror no SnapCenter . . . 17
Conceitos-chave de proteção de dados . . . 18
Sistemas de armazenamento e aplicativos suportados pelo SnapCenter . . . 20
Métodos de autenticação para credenciais do SnapCenter . . . 20
Operações SnapCenter suportadas para sistemas ASA r2 . . . 22
Início rápido para o SnapCenter software . . . 23
Instalar e configurar o SnapCenter Server . . . 24
Prepare-se para instalar o SnapCenter Server . . . 24
Requisitos para instalar o SnapCenter Server . . . 24
Registre-se para acessar o SnapCenter software . . . 30
Autenticação multifator (MFA) . . . 31
Instalar o SnapCenter Server . . . 41
Instalar o SnapCenter Server no host Windows . . . 41
Instalar o SnapCenter Server no host Linux . . . 45
Registrar SnapCenter . . . 49
Efetue login no SnapCenter usando autorização RBAC . . . 49
Configurar o SnapCenter Server . . . 53
Adicionar e provisionar o sistema de armazenamento . . . 53
Adicionar licenças baseadas no controlador SnapCenter Standard . . . 74
Configurar alta disponibilidade . . . 79
Configurar o controle de acesso baseado em função (RBAC) . . . 83
Configurar definições de log de auditoria . . . 112
Configurar conexões MySQL seguras com o SnapCenter Server . . . 113
Configurar autenticação baseada em certificado . . . 119
Habilitar autenticação baseada em certificado . . . 119
Exportar certificados de Autoridade Certificadora (CA) do SnapCenter Server . . . 120
Importar certificado CA para hosts de plug-in do Windows . . . 120
Importar certificado CA para hosts de plug-in UNIX . . . 121
Exportar certificados SnapCenter . . . 122
Configurar certificado CA para host Windows . . . 123
Gerar arquivo CSR de certificado CA . . . 123
Importar certificados de CA . . . 124

Obtenha a impressão digital do certificado CA . . . 124
Configurar certificado CA com serviços de plug-in de host do Windows . . . 125
Configurar certificado CA com o site SnapCenter . . . 126
Habilitar certificados CA para SnapCenter . . . 126
Configurar certificado CA para host Linux . . . 127
Configurar certificado nginx . . . 127
Configurar certificado de log de auditoria . . . 127
Configurar certificado de serviços do SnapCenter . . . 128
Configurar e habilitar a comunicação SSL bidirecional no host Windows . . . 128
Configurar comunicação SSL bidirecional no host Windows . . . 128
Habilitar comunicação SSL bidirecional no host Windows . . . 131
Configurar e habilitar comunicação SSL bidirecional no host Linux . . . 132
Configurar comunicação SSL bidirecional no host Linux . . . 132
Habilitar comunicação SSL no host Linux . . . 134
Configurar Active Directory, LDAP e LDAPS . . . 134
Registrar domínios não confiáveis do Active Directory . . . 134
Configurar pools de aplicativos do IIS para habilitar permissões de leitura do Active Directory . . . 136
Configurar certificado de cliente CA para LDAPS . . . 136
Proteja bancos de dados do Microsoft SQL Server . . . 138
Plug-in SnapCenter para Microsoft SQL Server . . . 138
Visão geral do plug-in SnapCenter para Microsoft SQL Server . . . 138
O que você pode fazer com o plug-in SnapCenter para Microsoft SQL Server . . . 138
Recursos do plug-in SnapCenter para Microsoft SQL Server . . . 139
Suporte para mapeamento assimétrico de LUN em clusters do Windows . . . 140
Tipos de armazenamento suportados pelo SnapCenter Plug-in para Microsoft SQL Server . . . 141
Recomendações de layout de armazenamento para o plug-in SnapCenter para Microsoft SQL Server 144
Privilégios ONTAP mínimos necessários para o plug-in SQL . . . 146
Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para Plug-in para servidor SQL . . . 148
Estratégia de backup para recursos do SQL Server . . . 149
Estratégia de restauração para SQL Server . . . 153
Definir uma estratégia de clonagem para o SQL Server . . . 157
Prepare-se para instalar o plug-in SnapCenter para Microsoft SQL Server . . . 157
Fluxo de trabalho de instalação do plug-in SnapCenter para Microsoft SQL Server . . . 157
Pré-requisitos para adicionar hosts e instalar o SnapCenter Plug-in para Microsoft SQL Server . . . 158
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows . . . 159
Configurar credenciais para o pacote de plug-ins do SnapCenter para Windows . . . 160
Configurar credenciais para um recurso individual do SQL Server . . . 162
Configurar o gMSA no Windows Server 2016 ou posterior . . . 164
Instalar o plug-in SnapCenter para Microsoft SQL Server . . . 165
Configurar certificado CA . . . 171
Configurar recuperação de desastres . . . 174
Instalar o SnapCenter Plug-in for VMware vSphere . . . 176
Implantar certificado CA . . . 177
Configurar o arquivo CRL . . . 177

Prepare-se para a proteção de dados . . . 177
Pré-requisitos para usar o SnapCenter Plug-in para Microsoft SQL Server . . . 177
Como recursos, grupos de recursos e políticas são usados para proteger o SQL Server . . . 178
Fazer backup do banco de dados, instância ou grupo de disponibilidade do SQL Server . . . 179
Fluxo de trabalho de backup . . . 179
Determinar se há recursos disponíveis para backup . . . 180
Migrar recursos para o sistema de armazenamento NetApp . . . 182
Crie políticas de backup para bancos de dados SQL Server . . . 183
Crie grupos de recursos e anexe políticas para o SQL Server . . . 190
Crie grupos de recursos e habilite a proteção secundária para recursos do Microsoft SQL Server em sistemas ASA r2 . . . 193
Requisitos para fazer backup de recursos SQL . . . 196
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell . . . 196
Fazer backup de recursos SQL . . . 197
Fazer backup de grupos de recursos do SQL Server . . . 203
Monitore as operações de backup de recursos SQL na página Tarefas do SnapCenter . . . 204
Cancelar o plug-in SnapCenter para operações de backup do Microsoft SQL Server . . . 205
Exibir backups e clones do SQL Server na página Topologia . . . 206
Limpe a contagem de backups secundários usando cmdlets do PowerShell . . . 208
Restaurar recursos do SQL Server . . . 208
Fluxo de trabalho de restauração . . . 208
Requisitos para restaurar um banco de dados . . . 209
Restaurar backups de banco de dados do SQL Server . . . 210
Restaurar um banco de dados SQL Server do armazenamento secundário . . . 217
Restaurar recursos usando cmdlets do PowerShell . . . 218
Bancos de dados do Grupo de Disponibilidade de Reseed . . . 220
Monitorar operações de restauração de recursos SQL . . . 221
Cancelar operações de restauração de recursos SQL . . . 222
Clonar recursos de banco de dados do SQL Server . . . 222
Fluxo de trabalho de clonagem . . . 222
Clonar de um backup de banco de dados SQL Server . . . 223
Executar ciclo de vida do clone . . . 231
Monitorar operações de clonagem de banco de dados SQL . . . 234
Cancelar operações de clonagem de recursos SQL . . . 235
Dividir um clone . . . 235
Proteja bancos de dados SAP HANA . . . 237
Plug-in SnapCenter para bancos de dados SAP HANA . . . 237
Visão geral do plug-in SnapCenter para banco de dados SAP HANA . . . 237
O que você pode fazer usando o plug-in SnapCenter para banco de dados SAP HANA . . . 237
Recursos do plug-in SnapCenter para banco de dados SAP HANA . . . 237
Tipos de armazenamento suportados pelo plug-in SnapCenter para banco de dados SAP HANA . . . 238
Privilégios mínimos do ONTAP necessários para o plug-in SAP HANA . . . 239
Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para bancos de dados SAP HANA . . . 242
Estratégia de backup para bancos de dados SAP HANA . . . 242

Estratégia de restauração e recuperação para bancos de dados SAP HANA . . . 246
Prepare-se para instalar o plug-in SnapCenter para banco de dados SAP HANA . . . 248
Fluxo de trabalho de instalação do plug-in SnapCenter para banco de dados SAP HANA . . . 248
Pré-requisitos para adicionar hosts e instalar o plug-in SnapCenter para banco de dados SAP HANA . . . 249
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows . . . 252
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux . . . 253
Configurar credenciais para o plug-in SnapCenter para banco de dados SAP HANA . . . 254
Configurar o gMSA no Windows Server 2016 ou posterior . . . 257
Instalar o plug-in SnapCenter para bancos de dados SAP HANA . . . 258
Configurar certificado CA . . . 264
Instalar o SnapCenter Plug-in for VMware vSphere . . . 271
Implantar certificado CA . . . 272
Configurar o arquivo CRL . . . 272
Prepare-se para a proteção de dados . . . 272
Pré-requisitos para usar o plug-in SnapCenter para banco de dados SAP HANA . . . 272
Como recursos, grupos de recursos e políticas são usados para proteger bancos de dados SAP HANA . . . 273
Fazer backup dos recursos do SAP HANA . . . 273
Fazer backup dos recursos do SAP HANA . . . 273
Configurar a chave de armazenamento do usuário HDB e o usuário do sistema operacional HDBSQL para o banco de dados SAP HANA . . . 274
Descubra recursos e prepare contêineres de banco de dados multilocatários para proteção de dados 275
Adicionar recursos manualmente ao host do plug-in . . . 278
Crie políticas de backup para bancos de dados SAP HANA . . . 279
Crie grupos de recursos e anexe políticas . . . 284
Crie grupos de recursos e habilite proteção secundária para recursos SAP HANA em sistemas ASA r2 . . . 288
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para o banco de dados SAP HANA . . . 291
Fazer backup de bancos de dados SAP HANA . . . 293
Fazer backup de grupos de recursos . . . 300
Monitorar operações de backup de bancos de dados SAP HANA . . . 300
Cancelar operações de backup para SAP HANA . . . 301
Visualize backups e clones do banco de dados SAP HANA na página Topologia . . . 302
Restaurar bancos de dados SAP HANA . . . 304
Fluxo de trabalho de restauração . . . 304
Restaurar e recuperar um backup de recurso adicionado manualmente . . . 305
Restaurar e recuperar um backup de banco de dados descoberto automaticamente . . . 309
Restaurar recursos usando cmdlets do PowerShell . . . 313
Monitorar operações de restauração de bancos de dados SAP HANA . . . 315
Clonar backups de recursos do SAP HANA . . . 316
Fluxo de trabalho de clonagem . . . 316
Clonar um backup de banco de dados SAP HANA . . . 317
Monitorar operações de clonagem de banco de dados SAP HANA . . . 320
Dividir um clone . . . 321

Excluir ou dividir clones de banco de dados SAP HANA após atualizar o SnapCenter . . . 322
Proteja bancos de dados Oracle . . . 324
Visão geral do plug-in SnapCenter para banco de dados Oracle . . . 324
O que você pode fazer com o Plug-in para Oracle Database . . . 324
Recursos do Plug-in para Oracle Database . . . 324
Tipos de armazenamento suportados pelo Plug-in para Oracle Database . . . 326
Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para Plug-in para Oracle . . . 328
Privilégios ONTAP mínimos necessários para o Plug-in para Oracle . . . 329
Instalar o plug-in SnapCenter para o banco de dados Oracle . . . 331
Fluxo de trabalho de instalação do plug-in SnapCenter para Oracle Database . . . 331
Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Linux ou AIX . . . 331
Adicionar hosts e instalar o pacote de plug-ins para Linux ou AIX usando a GUI . . . 340
Formas alternativas de instalar o pacote de plug-ins para Linux ou AIX . . . 344
Configurar o serviço SnapCenter Plug-in Loader . . . 347
Configurar certificado CA com o serviço SnapCenter Plug-in Loader (SPL) no host Linux . . . 350
Habilitar certificados CA para plug-ins . . . 353
Importar dados do SnapManager para Oracle e SnapManager para SAP para o SnapCenter . . . 353
Instalar o SnapCenter Plug-in for VMware vSphere . . . 359
Implantar certificado CA . . . 359
Configurar o arquivo CRL . . . 359
Prepare-se para proteger bancos de dados Oracle . . . 360
Fazer backup de bancos de dados Oracle . . . 361
Visão geral do procedimento de backup . . . 361
Informações de configuração de backup . . . 362
Requisitos para fazer backup de um banco de dados Oracle . . . 375
Descubra os bancos de dados Oracle disponíveis para backup . . . 375
Crie políticas de backup para bancos de dados Oracle . . . 377
Crie grupos de recursos e anexe políticas para bancos de dados Oracle . . . 384
Crie grupos de recursos e habilite proteção secundária para recursos Oracle em sistemas ASA r2 . . . 386
Fazer backup de recursos Oracle . . . 389
Fazer backup de grupos de recursos do banco de dados Oracle . . . 392
Monitorar backup do banco de dados Oracle . . . 393
Outras operações de backup . . . 394
Montar e desmontar backups de banco de dados . . . 398
Montar um backup de banco de dados . . . 398
Desmontar um backup de banco de dados . . . 400
Restaurar e recuperar bancos de dados Oracle . . . 400
Fluxo de trabalho de restauração . . . 400
Definir uma estratégia de restauração e recuperação para bancos de dados Oracle . . . 401
Variáveis de ambiente predefinidas para restaurar prescrições e postscripts específicos . . . 406
Requisitos para restaurar um banco de dados Oracle . . . 407
Restaurar e recuperar banco de dados Oracle . . . 408
Restaurar e recuperar tablespaces usando recuperação de ponto no tempo . . . 413
Restaurar e recuperar banco de dados plugável usando recuperação de ponto no tempo . . . 415

Restaurar e recuperar bancos de dados Oracle usando comandos UNIX . . . 417
Monitorar operações de restauração do banco de dados Oracle . . . 418
Cancelar operações de restauração do banco de dados Oracle . . . 418
Clonar banco de dados Oracle . . . 419
Fluxo de trabalho de clonagem . . . 419
Definir uma estratégia de clone para bancos de dados Oracle . . . 420
Variáveis de ambiente predefinidas para prescript e postscript específicos do clone . . . 421
Requisitos para clonar um banco de dados Oracle . . . 423
Clonar um backup de banco de dados Oracle . . . 425
Clonar um banco de dados plugável . . . 434
Clonar backups de banco de dados Oracle usando comandos UNIX . . . 439
Dividir um clone do banco de dados Oracle . . . 439
Clone dividido de um banco de dados plugável . . . 440
Monitorar operações de clonagem do banco de dados Oracle . . . 441
Atualizar um clone . . . 442
Excluir clone de um banco de dados plugável . . . 443
Gerenciar volumes de aplicativos . . . 443
O que são volumes de aplicação . . . 443
Adicionar volumes de aplicação . . . 444
Volumes de aplicativos de backup . . . 445
Clonar backup de volume do aplicativo . . . 447
Proteja os sistemas de arquivos do Windows . . . 450
Conceitos do plug-in SnapCenter para Microsoft Windows . . . 450
Visão geral do plug-in SnapCenter para Microsoft Windows . . . 450
O que você pode fazer com o plug-in SnapCenter para Microsoft Windows . . . 450
Recursos do plug-in SnapCenter para Windows . . . 451
Como o SnapCenter faz backup dos sistemas de arquivos do Windows . . . 452
Tipos de armazenamento suportados pelo SnapCenter Plug-in para Microsoft Windows . . . 452
Privilégios ONTAP mínimos necessários para o plug-in do Windows . . . 455
Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault . . . 457
Definir uma estratégia de backup para sistemas de arquivos do Windows . . . 458
Origens e destinos de clones para sistemas de arquivos do Windows . . . 460
Instalar o plug-in SnapCenter para Microsoft Windows . . . 460
Fluxo de trabalho de instalação do plug-in SnapCenter para Microsoft Windows . . . 460
Requisitos de instalação do plug-in SnapCenter para Microsoft Windows . . . 460
Adicionar hosts e instalar o plug-in SnapCenter para Microsoft Windows . . . 465
Instalar o plug-in SnapCenter para Microsoft Windows em vários hosts remotos usando cmdlets do PowerShell . . . 469
Instale o plug-in SnapCenter para Microsoft Windows silenciosamente a partir da linha de comando . . . 469
Monitorar o status de instalação do pacote de plug-in SnapCenter . . . 471
Configurar certificado CA . . . 472
Instalar o SnapCenter Plug-in for VMware vSphere . . . 475
Implantar certificado CA . . . 475
Configurar o arquivo CRL . . . 475
Fazer backup dos sistemas de arquivos do Windows . . . 475

Fazer backup dos sistemas de arquivos do Windows . . . 475
Determinar a disponibilidade de recursos para sistemas de arquivos do Windows . . . 477
Crie políticas de backup para sistemas de arquivos do Windows . . . 478
Criar grupos de recursos para sistemas de arquivos do Windows . . . 481
Crie grupos de recursos e habilite a proteção secundária para sistemas de arquivos do Windows em sistemas ASA r2 . . . 483
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell . . . 486
Fazer backup de um único recurso sob demanda para sistemas de arquivos do Windows . . . 487
Fazer backup de grupos de recursos para sistemas de arquivos do Windows . . . 491
Monitorar operações de backup . . . 492
Cancelar operações de backup . . . 493
Veja backups e clones relacionados na página Topologia . . . 494
Limpe a contagem de backups secundários usando cmdlets do PowerShell . . . 496
Restaurar sistemas de arquivos do Windows . . . 497
Restaurar backups do sistema de arquivos do Windows . . . 497
Restaurar recursos usando cmdlets do PowerShell . . . 502
Monitorar operações de restauração . . . 505
Cancelar operações de restauração . . . 506
Clonar sistemas de arquivos do Windows . . . 507
Clonar a partir de um backup do sistema de arquivos do Windows . . . 507
Monitorar operações de clonagem . . . 513
Cancelar operações de clonagem . . . 514
Dividir um clone . . . 515
Proteja os bancos de dados do Microsoft Exchange Server . . . 517
Conceitos do plug-in SnapCenter para Microsoft Exchange Server . . . 517
Visão geral do plug-in SnapCenter para Microsoft Exchange Server . . . 517
O que você pode fazer com o plug-in SnapCenter para Microsoft Exchange Server . . . 518
Tipos de armazenamento suportados pelo SnapCenter Plug-in para Microsoft Windows e para Microsoft Exchange Server . . . 518
Privilégios ONTAP mínimos necessários para o plug-in do Exchange . . . 519
Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault . . . 522
Definir uma estratégia de backup para recursos do Exchange Server . . . 522
Definir uma estratégia de restauração para bancos de dados do Exchange . . . 525
Instalar o plug-in SnapCenter para Microsoft Exchange Server . . . 526
Fluxo de trabalho de instalação do plug-in SnapCenter para Microsoft Exchange Server . . . 526
Pré-requisitos para adicionar hosts e instalar o SnapCenter Plug-in para Microsoft Exchange Server . . . 527
Configurar credenciais para o plug-in SnapCenter para Windows . . . 531
Configurar o gMSA no Windows Server 2016 ou posterior . . . 532
Adicionar hosts e instalar o Plug-in para Exchange . . . 534
Instalar o Plug-in para Exchange do host do SnapCenter Server usando cmdlets do PowerShell . . . 539
Instalar o plug-in SnapCenter para Exchange silenciosamente a partir da linha de comando . . . 539
Monitorar o status de instalação do pacote de plug-in SnapCenter . . . 541
Configurar certificado CA . . . 542
Configurar o SnapManager 7.x para que o Exchange e o SnapCenter coexistam . . . 545
Instalar o SnapCenter Plug-in for VMware vSphere . . . 547

Implantar certificado CA . . . 547
Configurar o arquivo CRL . . . 547
Prepare-se para a proteção de dados . . . 547
Pré-requisitos para usar o plug-in SnapCenter para Microsoft Exchange Server . . . 547
Como recursos, grupos de recursos e políticas são usados para proteger o Exchange Server . . . 548
Fazer backup dos recursos do Exchange . . . 549
Fluxo de trabalho de backup . . . 549
Banco de dados de troca e verificação de backup . . . 550
Determinar se os recursos do Exchange estão disponíveis para backup . . . 550
Criar políticas de backup para bancos de dados do Exchange Server . . . 552
Crie grupos de recursos e anexe políticas para servidores Exchange . . . 559
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para o Exchange Server . . . 562
Fazer backup de bancos de dados do Exchange . . . 563
Fazer backup de grupos de recursos do Exchange . . . 568
Monitorar operações de backup . . . 569
Cancelar operações de backup para banco de dados do Exchange . . . 570
Exibir backups do Exchange na página Topologia . . . 571
Restaurar recursos do Exchange . . . 573
Fluxo de trabalho de restauração . . . 573
Requisitos para restaurar um banco de dados do Exchange . . . 573
Restaurar bancos de dados do Exchange . . . 573
Recuperação granular de e-mails e caixas de correio . . . 578
Restaurar um banco de dados do Exchange Server a partir do armazenamento secundário . . . 578
Reproduzir uma réplica de nó passivo do Exchange . . . 579
Repropagar uma réplica usando cmdlets do PowerShell para banco de dados do Exchange . . . 580
Monitorar operações de restauração . . . 580
Cancelar operações de restauração para banco de dados do Exchange . . . 581
Proteja o IBM Db2 . . . 583
Plug-in SnapCenter para IBM Db2 . . . 583
Visão geral do plug-in SnapCenter para IBM Db2 . . . 583
O que você pode fazer usando o plug-in SnapCenter para IBM Db2 . . . 583
Recursos do plug-in SnapCenter para IBM Db2 . . . 584
Tipos de armazenamento suportados pelo SnapCenter Plug-in para IBM Db2 . . . 584
Privilégios ONTAP mínimos necessários para o plug-in IBM Db2 . . . 585
Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para IBM Db2 . . . 588
Estratégia de backup para IBM Db2 . . . 588
Estratégia de restauração e recuperação para IBM Db2 . . . 591
Prepare-se para instalar o plug-in SnapCenter para IBM Db2 . . . 592
Fluxo de trabalho de instalação do plug-in SnapCenter para IBM Db2 . . . 592
Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Windows, Linux ou AIX . . . 592
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows . . . 598
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux . . . 598
Configurar credenciais para o plug-in SnapCenter para IBM Db2 . . . 599
Configurar o gMSA no Windows Server 2016 ou posterior . . . 602

Instalar o plug-in SnapCenter para IBM Db2 . . . 603
Configurar certificado CA . . . 609
Prepare-se para a proteção de dados . . . 617
Pré-requisitos para usar o plug-in SnapCenter para IBM Db2 . . . 617
Como recursos, grupos de recursos e políticas são usados para proteger o IBM Db2 . . . 617
Fazer backup dos recursos do IBM Db2 . . . 618
Fazer backup dos recursos do IBM Db2 . . . 618
Descubra os bancos de dados automaticamente . . . 620
Adicionar recursos manualmente ao host do plug-in . . . 620
Criar políticas de backup para IBM Db2 . . . 622
Crie grupos de recursos e anexe políticas . . . 624
Crie grupos de recursos e habilite proteção secundária para recursos do IBM Db2 em sistemas ASA r2 . . . 628
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para IBM Db2 . . . 630
Fazer backup de bancos de dados Db2 . . . 632
Fazer backup de grupos de recursos . . . 639
Monitorar operações de backup do IBM Db2 . . . 640
Cancelar operações de backup para IBM Db2 . . . 641
Visualizar backups e clones do IBM Db2 na página Topologia . . . 642
Restaurar IBM Db2 . . . 644
Fluxo de trabalho de restauração . . . 644
Restaurar um backup de recurso adicionado manualmente . . . 644
Restaurar e recuperar um backup de banco de dados descoberto automaticamente . . . 649
Monitorar operações de restauração do IBM Db2 . . . 650
Clonar backups de recursos do IBM Db2 . . . 651
Fluxo de trabalho de clonagem . . . 651
Clonar um backup do IBM Db2 . . . 652
Monitorar operações de clone do IBM Db2 . . . 659
Dividir um clone . . . 660
Excluir ou dividir clones do banco de dados IBM Db2 após atualizar o SnapCenter . . . 661
Proteger PostgreSQL . . . 662
Plug-in SnapCenter para PostgreSQL . . . 662
Visão geral do plug-in SnapCenter para PostgreSQL . . . 662
O que você pode fazer usando o plug-in SnapCenter para PostgreSQL . . . 662
Recursos do plug-in SnapCenter para PostgreSQL . . . 662
Tipos de armazenamento suportados pelo SnapCenter Plug-in para PostgreSQL . . . 663
Privilégios ONTAP mínimos necessários para o plug-in PostgreSQL . . . 664
Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para PostgreSQL . . . 667
Estratégia de backup para PostgreSQL . . . 667
Estratégia de restauração e recuperação para PostgreSQL . . . 670
Prepare-se para instalar o plug-in SnapCenter para PostgreSQL . . . 671
Fluxo de trabalho de instalação do plug-in SnapCenter para PostgreSQL . . . 671
Pré-requisitos para adicionar hosts e instalar o plug-in SnapCenter para PostgreSQL . . . 672
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows . . . 675

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux . . . 676
Configurar credenciais para o plug-in SnapCenter para PostgreSQL . . . 677
Configurar o gMSA no Windows Server 2016 ou posterior . . . 680
Instalar o plug-in SnapCenter para PostgreSQL . . . 681
Configurar certificado CA . . . 687
Prepare-se para a proteção de dados . . . 695
Pré-requisitos para usar o plug-in SnapCenter para PostgreSQL . . . 695
Como recursos, grupos de recursos e políticas são usados para proteger o PostgreSQL . . . 695
Fazer backup dos recursos do PostgreSQL . . . 696
Fazer backup dos recursos do PostgreSQL . . . 696
Descubra os clusters automaticamente . . . 698
Adicionar recursos manualmente ao host do plug-in . . . 698
Criar políticas de backup para PostgreSQL . . . 700
Crie grupos de recursos e anexe políticas . . . 703
Crie grupos de recursos e habilite proteção secundária para recursos do PostgreSQL em sistemas ASA r2 . . . 707
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para PostgreSQL . . . 709
Fazer backup do PostgreSQL . . . 711
Fazer backup de grupos de recursos . . . 716
Monitorar operações de backup do PostgreSQL . . . 717
Cancelar operações de backup para PostgreSQL . . . 718
Visualizar backups e clones do PostgreSQL na página Topologia . . . 719
Restaurar PostgreSQL . . . 720
Fluxo de trabalho de restauração . . . 720
Restaurar e recuperar um backup de recurso adicionado manualmente . . . 721
Restaurar e recuperar um backup de cluster descoberto automaticamente . . . 725
Restaurar recursos usando cmdlets do PowerShell . . . 727
Monitorar operações de restauração do PostgreSQL . . . 730
Clonar backups de recursos do PostgreSQL . . . 731
Fluxo de trabalho de clonagem . . . 731
Clonar um backup do PostgreSQL . . . 732
Monitorar operações de clonagem do PostgreSQL . . . 735
Dividir um clone . . . 736
Excluir ou dividir clones de cluster do PostgreSQL após atualizar o SnapCenter . . . 737
Proteger MySQL . . . 739
Plug-in SnapCenter para MySQL . . . 739
Visão geral do plug-in SnapCenter para MySQL . . . 739
O que você pode fazer usando o plug-in SnapCenter para MySQL . . . 739
Recursos do plug-in SnapCenter para MySQL . . . 739
Tipos de armazenamento suportados pelo SnapCenter Plug-in para MySQL . . . 740
Privilégios ONTAP mínimos necessários para o plug-in MySQL . . . 741
Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para MySQL . . . 744
Estratégia de backup para MySQL . . . 744
Estratégia de restauração e recuperação para MySQL . . . 747

Prepare-se para instalar o plug-in SnapCenter para MySQL . . . 748
Fluxo de trabalho de instalação do plug-in SnapCenter para MySQL . . . 748
Pré-requisitos para adicionar hosts e instalar o SnapCenter Plug-in para MySQL . . . 748
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows . . . 752
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux . . . 752
Configurar credenciais para o plug-in SnapCenter para MySQL . . . 753
Instalar o plug-in SnapCenter para MySQL . . . 756
Configurar certificado CA . . . 761
Prepare-se para a proteção de dados . . . 769
Pré-requisitos para usar o plug-in SnapCenter para MySQL . . . 769
Como recursos, grupos de recursos e políticas são usados para proteger o MySQL . . . 769
Fazer backup dos recursos do MySQL . . . 770
Fazer backup dos recursos do MySQL . . . 770
Descubra os bancos de dados automaticamente . . . 772
Adicionar recursos manualmente ao host do plug-in . . . 772
Criar políticas de backup para MySQL . . . 773
Crie grupos de recursos e anexe políticas . . . 777
Crie grupos de recursos e habilite proteção secundária para recursos MySQL em sistemas ASA r2 . . . 781
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para MySQL . . . 783
Fazer backup do MySQL . . . 785
Fazer backup de grupos de recursos . . . 791
Monitorar operações de backup do MySQL . . . 792
Cancelar operações de backup para MySQL . . . 793
Visualize backups e clones do MySQL na página Topologia . . . 794
Restaurar MySQL . . . 795
Fluxo de trabalho de restauração . . . 795
Restaurar e recuperar um backup de recurso adicionado manualmente . . . 796
Restaurar e recuperar um backup de banco de dados descoberto automaticamente . . . 800
Restaurar recursos usando cmdlets do PowerShell . . . 802
Monitorar operações de restauração do MySQL . . . 804
Clonar backups de recursos do MySQL . . . 805
Fluxo de trabalho de clonagem . . . 805
Clonar um backup do MySQL . . . 806
Monitorar operações de clonagem do MySQL . . . 809
Dividir um clone . . . 810
Excluir ou dividir clones de banco de dados MySQL após atualizar o SnapCenter . . . 811
Proteja aplicativos usando plug-ins compatíveis com NetApp . . . 812
Plug-ins suportados pela NetApp . . . 812
Visão geral dos plug-ins suportados pela NetApp . . . 812
O que você pode fazer com os plug-ins suportados pela NetApp . . . 812
Recursos de plug-ins suportados pela NetApp . . . 813
Tipos de armazenamento suportados pelos plug-ins suportados pela NetApp . . . 814
Privilégios ONTAP mínimos necessários para plug-in compatível com NetApp . . . 814
Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para plug-ins

compatíveis com NetApp . . . 817
Definir uma estratégia de backup . . . 817
Estratégia de backup para plug-ins suportados pela NetApp . . . 818
Tipos de estratégias de restauração suportadas para recursos de plug-in suportados pela NetApp adicionados manualmente . . . 819
Prepare-se para instalar plug-ins compatíveis com NetApp . . . 819
Fluxo de trabalho de instalação de plug-ins compatíveis com SnapCenter NetApp . . . 819
Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Windows, Linux ou AIX . . . 820
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows . . . 824
Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux e AIX . . . 825
Configurar credenciais para plug-ins compatíveis com NetApp . . . 826
Configurar o gMSA no Windows Server 2016 ou posterior . . . 829
Instalar os plug-ins suportados pela NetApp . . . 830
Configurar certificado CA . . . 836
Prepare-se para a proteção de dados . . . 844
Pré-requisitos para usar os plug-ins suportados pela NetApp . . . 844
Como recursos, grupos de recursos e políticas são usados para proteger recursos de plug-in com suporte da NetApp . . . 845
Faça backup dos recursos de plug-ins suportados pela NetApp . . . 845
Faça backup dos recursos de plug-ins suportados pela NetApp . . . 845
Adicionar recursos aos plug-ins suportados pela NetApp . . . 846
Criar políticas para recursos de plug-in suportados NetApp . . . 850
Crie grupos de recursos e anexe políticas . . . 854
Crie grupos de recursos e habilite proteção secundária para recursos em sistemas ASA r2 . . . 858
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell . . . 860
Faça backup de recursos individuais de plug-ins suportados pela NetApp . . . 861
Fazer backup de grupos de recursos de plug-ins suportados NetApp . . . 867
Monitorar operações de backup de recursos de plug-in com suporte da NetApp . . . 868
Cancelar operações de backup para plug-ins compatíveis com NetApp . . . 869
Exibir backups e clones relacionados a recursos de plug-ins suportados pela NetApp na página Topologia . . . 870
Restaurar recursos de plug-ins suportados pela NetApp . . . 871
Restaurar recursos de plug-in suportados pelo NetApp . . . 871
Restaurar um backup de recurso . . . 872
Monitorar operações de restauração de recursos de plug-in suportados NetApp . . . 876
Clonar backups de recursos de plug-ins suportados pelo NetApp . . . 877
Clonar backups de recursos de plug-ins suportados pelo NetApp . . . 877
Clonar de um backup . . . 878
Monitorar operações de clonagem de recursos de plug-in com suporte do NetApp . . . 884
Proteja os sistemas de arquivos Unix . . . 886
O que você pode fazer com o plug-in SnapCenter para sistemas de arquivos Unix . . . 886
Configurações suportadas . . . 886
Limitações . . . 887
Características . . . 887
Instalar o plug-in SnapCenter para sistemas de arquivos Unix . . . 887

Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Linux . . . 887
Adicionar hosts e instalar o pacote de plug-ins para Linux usando a GUI . . . 889
Configurar o serviço SnapCenter Plug-in Loader . . . 892
Configurar certificado CA com o serviço SnapCenter Plug-in Loader (SPL) no host Linux . . . 895
Habilitar certificados CA para plug-ins . . . 898
Instalar o SnapCenter Plug-in for VMware vSphere . . . 898
Implantar certificado CA . . . 898
Configurar o arquivo CRL . . . 899
Prepare-se para proteger sistemas de arquivos Unix . . . 899
Fazer backup de sistemas de arquivos Unix . . . 899
Descubra os sistemas de arquivos UNIX disponíveis para backup . . . 899
Crie políticas de backup para sistemas de arquivos Unix . . . 900
Crie grupos de recursos e anexe políticas para sistemas de arquivos Unix . . . 903
Crie grupos de recursos e habilite proteção secundária para sistemas de arquivos Unix em sistemas ASA r2 . . . 905
Fazer backup de sistemas de arquivos Unix . . . 907
Fazer backup de grupos de recursos de sistemas de arquivos Unix . . . 909
Monitorar backup de sistemas de arquivos Unix . . . 909
Exibir sistemas de arquivos Unix protegidos na página Topologia . . . 911
Restaurar e recuperar sistemas de arquivos Unix . . . 913
Restaurar sistemas de arquivos Unix . . . 913
Monitorar operações de restauração de sistemas de arquivos Unix . . . 914
Clonar sistemas de arquivos Unix . . . 915
Clonar backup do sistema de arquivos Unix . . . 915
Dividir um clone . . . 916
Monitorar operações de clonagem de sistemas de arquivos Unix . . . 918
Proteja aplicativos em execução no Azure NetApp Files . . . 919
Proteja aplicativos em execução no Azure NetApp Files . . . 919
Limitações . . . 919
Instale o SnapCenter e crie credenciais . . . 919
Instalar o SnapCenter na Máquina Virtual do Azure . . . 919
Crie a credencial do Azure no SnapCenter . . . 921
Configurar a conta de armazenamento do Azure . . . 922
Crie a credencial para adicionar o host do plug-in . . . 922
Proteja bancos de dados SAP HANA . . . 923
Adicionar hosts e instalar o plug-in SnapCenter para o banco de dados SAP HANA . . . 923
Adicionar banco de dados SAP HANA . . . 924
Crie políticas de backup para bancos de dados SAP HANA . . . 924
Crie grupos de recursos e anexe políticas de backup do SAP HANA . . . 925
Fazer backup de bancos de dados SAP HANA em execução no Azure NetApp Files . . . 926
Fazer backup de grupos de recursos do SAP HANA . . . 927
Restaurar e recuperar bancos de dados SAP HANA . . . 927
Clonar backup de banco de dados SAP HANA . . . 928
Proteja bancos de dados do Microsoft SQL Server . . . 929
Adicionar hosts e instalar o plug-in SnapCenter para banco de dados SQL Server . . . 929

Crie políticas de backup para bancos de dados SQL Server . . . 930
Crie grupos de recursos e anexe políticas de backup SQL . . . 932
Fazer backup de bancos de dados do SQL Server em execução no Azure NetApp Files . . . 933
Fazer backup de grupos de recursos do SQL Server . . . 934
Restaurar e recuperar bancos de dados SQL Server . . . 934
Clonar backup do banco de dados SQL Server . . . 935
Proteja bancos de dados Oracle . . . 937
Adicionar hosts e instalar o plug-in SnapCenter para banco de dados Oracle . . . 937
Crie políticas de backup para bancos de dados Oracle . . . 938
Crie grupos de recursos e anexe políticas de backup do Oracle . . . 938
Fazer backup de bancos de dados Oracle em execução no Azure NetApp Files . . . 940
Fazer backup de grupos de recursos Oracle . . . 940
Restaurar e recuperar bancos de dados Oracle . . . 941
Clonar backup do banco de dados Oracle . . . 943
Gerenciar SnapCenter Server e plug-ins . . . 947
Ver painel . . . 947
Visão geral do painel . . . 947
Como visualizar informações no painel . . . 951
Solicitar relatórios de status dos trabalhos no painel . . . 951
Solicitar relatórios do status de proteção no painel . . . 952
Gerenciar RBAC . . . 952
Modificar uma função . . . 952
Modificar usuários e grupos . . . 953
Gerenciar hosts . . . 953
Atualizar informações da máquina virtual . . . 955
Modificar hosts de plug-in . . . 956
Iniciar ou reiniciar serviços de plug-in . . . 957
Suspender agendamentos para manutenção do host . . . 957
Operações suportadas pela página de Recursos . . . 958
Gerenciar políticas . . . 959
Modificar políticas . . . 959
Políticas de desanexação . . . 960
Excluir políticas . . . 960
Gerenciar grupos de recursos . . . 960
Parar e retomar operações em grupos de recursos . . . 961
Excluir grupos de recursos . . . 961
Gerenciar backups . . . 961
Renomear backups . . . 962
Excluir backups . . . 962
Remover proteção . . . 963
Excluir clones . . . 963
Monitorar trabalhos, agendamentos, eventos e registros . . . 964
Monitorar trabalhos . . . 964
Monitorar cronogramas . . . 965
Monitorar eventos . . . 965

Registros de monitoramento . . . 966
Remover trabalhos e logs do SnapCenter . . . 967
Visão geral dos recursos de relatórios do SnapCenter . . . 967
Relatórios de acesso . . . 969
Filtre seu relatório . . . 969
Exportar ou imprimir relatórios . . . 970
Defina o servidor SMTP para notificações por e-mail . . . 970
Configurar a opção de enviar relatórios por e-mail . . . 970
Gerenciar o repositório do SnapCenter Server . . . 971
Pré-requisitos para proteger o repositório SnapCenter . . . 971
Faça backup do repositório SnapCenter . . . 971
Ver backups do repositório SnapCenter . . . 972
Restaurar o repositório do banco de dados SnapCenter . . . 972
Migrar o repositório SnapCenter . . . 973
Redefinir a senha do repositório SnapCenter . . . 973
Gerenciar recursos de domínios não confiáveis . . . 974
Modificar domínios não confiáveis . . . 974
Cancelar registro de domínios não confiáveis do Active Directory . . . 975
Gerenciar o sistema de armazenamento . . . 975
Modificar a configuração do sistema de armazenamento . . . 976
Excluir o sistema de armazenamento . . . 978
Suporte à API REST . . . 979
Gerenciar coleta de dados de EMS . . . 979
Interrompa a coleta de dados do EMS . . . 979
Iniciar coleta de dados do EMS . . . 980
Alterar cronograma de coleta de dados do EMS e SVM de destino . . . 980
Monitorar o status da coleta de dados do EMS . . . 980
Atualizar o SnapCenter Server e os plug-ins . . . 982
Configure o SnapCenter para verificar se há atualizações disponíveis . . . 982
Fluxo de trabalho de atualização . . . 982
Caminhos de atualização suportados . . . 982
Atualizar o SnapCenter Server no host Windows . . . 983
Atualizar o SnapCenter Server no host Linux . . . 985
Atualize seus pacotes de plug-ins . . . 986
Atualização tecnológica . . . 989
Atualização tecnológica do host do SnapCenter Server . . . 989
Atualização tecnológica de um nó no cluster F5 . . . 990
Desativando o antigo host do SnapCenter Server . . . 990
Reverter para o antigo host do SnapCenter Server . . . 990
Recuperação de desastres . . . 990
Atualização tecnológica dos hosts de plug-in SnapCenter . . . 992
Atualização tecnológica do sistema de armazenamento . . . 994
Atualizar os backups do armazenamento primário . . . 995
Atualizar os backups do armazenamento secundário . . . 997
Desinstalar o SnapCenter Server e os plug-ins . . . 999

Desinstalar pacotes de plug-in SnapCenter . . . 999
Pré-requisitos para remover um host . . . 999
Remover um host . . . 1000
Desinstalar plug-ins usando a interface gráfica do usuário do SnapCenter . . . 1000
Desinstalar plug-ins do Windows usando o cmdlet do PowerShell . . . 1001
Desinstalar plug-ins localmente em um host . . . 1002
Desinstalar pacote de plug-ins para Linux ou AIX usando CLI . . . 1002
Desinstalar o SnapCenter Server no host Windows . . . 1003
Desinstalar o SnapCenter Server no host Linux . . . 1003
Automatize usando APIs REST . . . 1005
Automação do SnapCenter usando APIs REST . . . 1005
Como acessar a API REST do SnapCenter nativamente . . . 1005
Fundação de serviços web REST . . . 1005
Recursos e representação estatal . . . 1005
Pontos finais de URI . . . 1006
Mensagens HTTP . . . 1006
Formatação JSON . . . 1006
Características operacionais básicas . . . 1006
Transação de API de solicitação e resposta . . . 1006
Suporte para operações CRUD . . . 1006
Identificadores de objetos . . . 1007
Instâncias e coleções de objetos . . . 1007
Operações síncronas e assíncronas . . . 1007
Segurança . . . 1007
Variáveis de entrada que controlam uma solicitação de API . . . 1008
Métodos HTTP . . . 1008
Cabeçalhos de solicitação . . . 1008
Corpo da solicitação . . . 1008
Filtrando objetos . . . 1009
Solicitando campos de objetos específicos . . . 1009
Classificando objetos no conjunto de saída . . . 1010
Paginação ao recuperar objetos em uma coleção . . . 1010
Propriedades de tamanho . . . 1011
Interpretação de uma resposta de API . . . 1011
Código de status HTTP . . . 1011
Cabeçalhos de resposta . . . 1012
Corpo de resposta . . . 1012
Erros . . . 1013
APIs REST suportadas pelo SnapCenter Server e plug-ins . . . 1014
Aut. . . . 1014
Domínios . . . 1014
Empregos . . . 1014
Configurações . . . 1014
Anfitriões . . . 1015
Recursos . . . 1015

Backups . . . 1017
Clones . . . 1017
Divisão do clone . . . 1017
Grupos de Recursos . . . 1017
Políticas . . . 1018
Armazenar . . . 1018
Compartilhar . . . 1018
Plugins . . . 1019
Relatórios . . . 1020
Alertas . . . 1020
RBAC . . . 1020
Configuração . . . 1020
Configurações do Certificado . . . 1021
Repositório . . . 1021
Versão . . . 1021
Como acessar APIs REST usando a página da web da API do Swagger . . . 1021
Comece a usar a API REST . . . 1022
Olá Mundo . . . 1022
Avisos legais . . . 1023
Direitos autorais . . . 1023
Marcas Registradas . . . 1023
Patentes . . . 1023
Política de Privacidade . . . 1023
Código aberto . . . 1023

Documentação do SnapCenter software

Notas de lançamento

Notas de lançamento

Saiba mais sobre os novos e aprimorados recursos disponíveis no SnapCenter 6.1.

Para obter uma lista completa de novos recursos e aprimoramentos, consulte "Novidades no SnapCenter 6.1" .

Para obter detalhes sobre problemas conhecidos, limitações, problemas corrigidos e comandos novos e alterados, consulte o "Notas de versão do software SnapCenter 6.1" . Você deve entrar com sua conta NetApp ou criar uma conta para acessar as Notas de Versão.

Caminhos de atualização suportados para SnapCenter

O caminho de atualização ajuda você a entender quais versões anteriores do SnapCenter você pode atualizar para as versões mais recentes do SnapCenter e quais versões dos plug-ins são suportadas.

Se você estiver na versão SnapCenter Server…	Você pode atualizar diretamente o SnapCenter Server para…	Versões de plug-in suportadas
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

Para obter informações sobre como atualizar o SnapCenter Plug-in for VMware vSphere, consulte "Atualizar o SnapCenter Plug-in for VMware vSphere" .

Começar

Saiba mais sobre o SnapCenter software

Visão geral do SnapCenter

O SnapCenter software é uma plataforma simples, centralizada e escalável para proteção de dados consistente com aplicativos. Ele protege aplicativos, bancos de dados, sistemas de arquivos host e VMs em sistemas ONTAP na Nuvem Híbrida.

O SnapCenter usa as tecnologias NetApp Snapshot, SnapRestore, FlexClone, SnapMirror e SnapVault para fornecer:

- Backups rápidos, com eficiência de espaço, consistentes com o aplicativo e baseados em disco
- Restauração rápida e detalhada e recuperação consistente com o aplicativo
- Clonagem rápida e com economia de espaço

O SnapCenter inclui o SnapCenter Server e plug-ins leves. Você pode automatizar a implantação de plug-ins em hosts de aplicativos remotos, agendar operações de backup, verificação e clonagem, além de monitorar operações de proteção de dados.

Você pode instalar o SnapCenter no local ou em uma nuvem pública para proteger dados.

- No local para proteger o seguinte:
  - Dados que estão nos sistemas primários ONTAP FAS, AFF ou ASA e replicados para os sistemas secundários ONTAP FAS, AFF ou ASA
  - Dados que estão nos sistemas primários ONTAP Select
  - Dados que estão nos sistemas primários e secundários ONTAP FAS, AFF ou ASA e protegidos no armazenamento de objetos StorageGRID local
  - Dados que estão nos sistemas primário e secundário ONTAP ASA r2
- No local em uma Nuvem Híbrida para proteger o seguinte:
  - Dados que estão nos sistemas primários ONTAP FAS, AFF ou ASA e replicados para o Cloud Volumes ONTAP
  - Dados que estão nos sistemas primários e secundários ONTAP FAS, AFF ou ASA e protegidos para armazenamento de objetos e arquivos na nuvem (usando a integração de BlueXP backup and recovery)
- Em uma nuvem pública para proteger o seguinte:
  - Dados que estão nos sistemas primários do Cloud Volumes ONTAP (anteriormente ONTAP Cloud)
  - Dados que estão no Amazon FSX para ONTAP
  - Dados que estão nos Azure NetApp Files (Oracle, Microsoft SQL e SAP HANA)

Principais características

O SnapCenter oferece os seguintes recursos principais:

- Proteção de dados centralizada e consistente com a aplicação de diferentes aplicações

A proteção de dados é suportada pelo Microsoft Exchange Server, Microsoft SQL Server, Oracle Databases no Linux ou AIX, banco de dados SAP HANA, IBM Db2, PostgreSQL, MySQL e Windows Host Filesystems executados em sistemas ONTAP . O SnapCenter também oferece suporte à proteção de aplicativos como MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM.

- Backups baseados em políticas

  Os backups baseados em políticas aproveitam a tecnologia NetApp Snapshot para criar backups rápidos, com eficiência de espaço e consistentes com aplicativos, baseados em disco. Você também pode configurar a proteção automática desses backups para armazenamento secundário atualizando os relacionamentos de proteção existentes.

- Backups para vários recursos

  Você pode fazer backup de vários recursos (aplicativos, bancos de dados ou sistemas de arquivos host) do mesmo tipo ao mesmo tempo usando grupos de recursos do SnapCenter .

- Restauração e recuperação

  O SnapCenter fornece restaurações rápidas e granulares de backups e recuperação consistente com o aplicativo e baseada em tempo. Você pode restaurar de qualquer destino na Nuvem Híbrida.

- Clonagem

  O SnapCenter oferece clonagem rápida, com economia de espaço e consistente com o aplicativo. Você pode clonar em qualquer destino na Nuvem Híbrida.

- Interface gráfica de usuário de gerenciamento de usuário único

  O SnapCenter fornece uma interface única para gerenciar backups e clones em qualquer destino de Nuvem Híbrida.

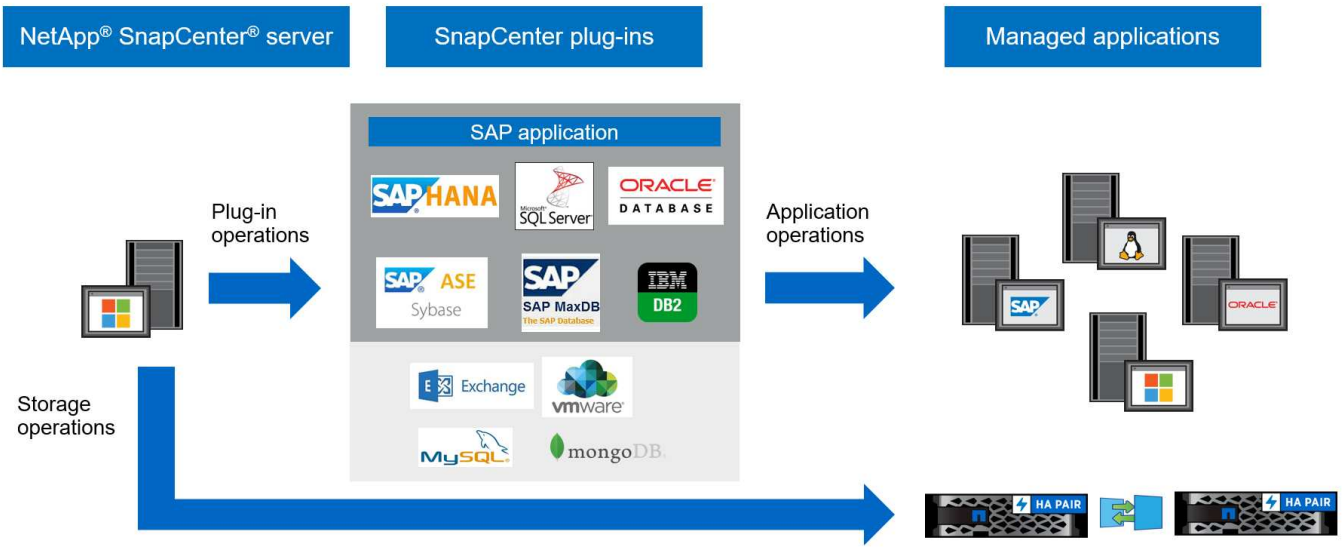
- APIs REST, cmdlets do Windows, comandos UNIX

  O SnapCenter fornece APIs REST para a maioria das funcionalidades para integração com qualquer software de orquestração e uso de cmdlets do Windows PowerShell e interface de linha de comando.

- Painel e relatórios centralizados de proteção de dados
- Controle de acesso baseado em função (RBAC) para segurança e delegação
- Um banco de dados de repositório integrado com alta disponibilidade para armazenar todos os metadados de backup
- Instalação automática de plug-ins
- Alta disponibilidade
- Recuperação de Desastres (DR)
- SnapLock "Saber mais"
- Sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC])
- Espelhamento síncrono "Saber mais"

Arquitetura e componentes do SnapCenter

O SnapCenter usa um design em camadas com um servidor de gerenciamento central e hosts de plug-in. Os hosts do servidor e do plug-in podem estar em locais diferentes.



O SnapCenter inclui o SnapCenter Server, o pacote SnapCenter Plug-in para Windows e o pacote SnapCenter Plug-In para Linux. Cada pacote contém plug-ins para vários aplicativos e componentes de infraestrutura.

Servidor SnapCenter

O SnapCenter Server oferece suporte aos sistemas operacionais Microsoft Windows e Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5). O servidor SnapCenter inclui um servidor web, uma interface de usuário centralizada baseada em HTML5, cmdlets do PowerShell, APIs REST e o repositório SnapCenter .

O SnapCenter armazena informações sobre suas operações no repositório SnapCenter .

Plug-ins do SnapCenter

Cada plug-in do SnapCenter oferece suporte a ambientes, bancos de dados e aplicativos específicos.

Nome do plug-in	Incluído no pacote de instalação	Requer outros plug-ins	Instalado no host	Plataforma suportada
Plug-in SnapCenter para Microsoft SQL Server	Pacote de plug-ins para Windows	Plug-in para Windows	Host do SQL Server	Windows
Plug-in SnapCenter para Windows	Pacote de plug-ins para Windows		Host do Windows	Windows
Plug-in SnapCenter para Microsoft Exchange Server	Pacote de plug-ins para Windows	Plug-in para Windows	Host do Exchange Server	Windows
Plug-in SnapCentre para Oracle Database	Pacote de plug-ins para Linux e pacote de plug-ins para AIX	Plug-in para UNIX	Host Oracle	Linux ou AIX

Nome do plug-in	Incluído no pacote de instalação	Requer outros plug-ins	Instalado no host	Plataforma suportada
Plug-in SnapCenter para banco de dados SAP HANA	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host do cliente HDBSQL	Linux ou Windows
Plug-in SnapCenter para IBM Db2	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host Db2	Linux, AIX ou Windows
Plug-in SnapCenter para PostgreSQL	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host PostgreSQL	Linux ou Windows
Plug-in SnaoCenter para MySQL	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou Plug-in para Windows	Host MySQL	Linux ou Windows
Plug-in SnapCenter para MongoDB	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host MongoDB	Linux ou Windows
Plug-in SnapCenter para ORASCPM (Aplicativos Oracle)	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host Oracle	Linux ou Windows
Plug-in SnapCenter para SAP ASE	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host SAP	Linux ou Windows
Plug-in SnapCenter para SAP MaxDB	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host SAP MaxDB	Linux ou Windows
Plug-in SnapCenter para plug-in de armazenamento	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou plug-in para Windows	Host de armazenamento	Linux ou Windows

O SnapCenter Plug-in for VMware vSphere oferece suporte a operações de backup e restauração consistentes em caso de falhas e em VMs para máquinas virtuais (VMs), armazenamentos de dados e discos

de máquina virtual (VMDKs). Ele também oferece suporte a operações de backup e restauração consistentes com aplicativos para bancos de dados virtualizados e sistemas de arquivos.

Para proteger bancos de dados, sistemas de arquivos, VMs ou armazenamentos de dados em VMs, implante o SnapCenter Plug-in for VMware vSphere . Para obter informações, consulte "Documentação do SnapCenter Plug-in for VMware vSphere" .

Repositório SnapCenter

O repositório SnapCenter , às vezes chamado de banco de dados NSM, armazena informações e metadados para cada operação do SnapCenter .

A instalação do SnapCenter Server instala o banco de dados do repositório do MySQL Server por padrão. Se você já instalou o MySQL Server e deseja executar uma nova instalação do SnapCenter Server, desinstale o MySQL Server.

O SnapCenter suporta o MySQL Server 8.0.37 ou posterior como banco de dados de repositório do SnapCenter . Se você usar uma versão anterior do MySQL Server com uma versão anterior do SnapCenter, o processo de atualização do SnapCenter atualizará o MySQL Server para a versão 8.0.37 ou posterior.

O repositório SnapCenter armazena as seguintes informações e metadados:

- Backup, clonagem, restauração e verificação de metadados
- Relatórios, informações sobre empregos e eventos
- Informações de host e plug-in
- Detalhes de função, usuário e permissão
- Informações de conexão do sistema de armazenamento

Recursos de segurança no SnapCenter

O SnapCenter emprega recursos rigorosos de segurança e autenticação para permitir que você mantenha seus dados seguros.

O SnapCenter inclui os seguintes recursos de segurança:

- Toda a comunicação com o SnapCenter usa HTTP sobre SSL (HTTPS).
- Todas as credenciais no SnapCenter são protegidas usando criptografia Advanced Encryption Standard (AES).
- Suporta algoritmos de segurança compatíveis com o Padrão Federal de Processamento de Informações (FIPS).
- Suporta o uso de certificados de CA autorizados fornecidos pelo cliente.
- Suporta Transport Layer Security (TLS) 1.3 para comunicação com ONTAP. Você também pode usar o TLS 1.2 para comunicação entre clientes e servidores.
- Oferece suporte a um determinado conjunto de conjuntos de cifras SSL para fornecer segurança na comunicação de rede. "Saber mais" .
- O SnapCenter é instalado dentro do firewall da sua empresa para permitir o acesso ao SnapCenter Server e permitir a comunicação entre o SnapCenter Server e os plug-ins.
- O acesso à API e à operação do SnapCenter usa tokens criptografados com criptografia AES, que expiram após 24 horas.

- O SnapCenter integra-se ao Windows Active Directory para login e controle de acesso baseado em função (RBAC) que controlam as permissões de acesso.
- O IPsec é compatível com o SnapCenter no ONTAP para máquinas host Windows e Linux. "Saber mais" .
- Os cmdlets do SnapCenter PowerShell são protegidos por sessão.
- Após um período padrão de 15 minutos de inatividade, o SnapCenter avisa que você será desconectado em 5 minutos.

  Após 20 minutos de inatividade, o SnapCenter desconecta você e você deve efetuar login novamente. Você pode modificar o período de logout.

- O login é temporariamente desativado após 5 tentativas incorretas de login.
- Suporta autenticação de certificado CA entre SnapCenter Server e ONTAP. "Saber mais" .
- O Integrity Verifier é adicionado ao SnapCenter Server e aos plug-ins e valida todos os binários enviados durante novas operações de instalação e atualização.

Visão geral do certificado CA

O instalador do SnapCenter Server habilita o suporte ao certificado SSL centralizado durante a instalação. Para melhorar a comunicação segura entre o servidor e o plug-in, o SnapCenter oferece suporte ao uso de certificados de CA autorizados fornecidos pelo cliente.

Você deve implantar certificados de CA após instalar o SnapCenter Server e os respectivos plug-ins. Para obter mais informações, consulte "Gerar arquivo CSR de certificado CA" .

Você também pode implantar o certificado CA para o plug-in SnapCenter para VMware vSphere. Para obter mais informações, consulte "Criar e importar certificados" .

Comunicação SSL bidirecional

A comunicação SSL bidirecional protege a comunicação mútua entre o SnapCenter Server e os plug-ins.

Visão geral da autenticação baseada em certificado

A autenticação baseada em certificado verifica a autenticidade dos respectivos usuários que tentam acessar o host do plug-in SnapCenter . O usuário deve exportar o certificado do SnapCenter Server sem a chave privada e importá-lo no armazenamento confiável do host do plug-in. A autenticação baseada em certificado funciona somente se o recurso SSL bidirecional estiver habilitado.

Autenticação multifator (MFA)

O MFA usa um Provedor de Identidade (IdP) de terceiros por meio da Linguagem de Marcação de Asserção de Segurança (SAML) para gerenciar sessões de usuários. Essa funcionalidade aumenta a segurança da autenticação ao oferecer a opção de usar vários fatores, como TOTP, biometria, notificações push etc., juntamente com o nome de usuário e a senha existentes. Além disso, ele permite que o cliente use seus próprios provedores de identidade de usuário para obter login de usuário unificado (SSO) em todo o seu portfólio.

O MFA é aplicável somente ao login da interface de usuário do SnapCenter Server. Os logins são autenticados por meio do IdP Active Directory Federation Services (AD FS). Você pode configurar vários fatores de autenticação no AD FS. O SnapCenter é o provedor de serviços e você deve configurar o SnapCenter como uma parte confiável no AD FS. Para habilitar o MFA no SnapCenter, você precisará dos metadados do AD FS.

Para obter informações sobre como habilitar o MFA, consulte"Habilitar autenticação multifator" .

Controle de acesso baseado em função no SnapCenter

O controle de acesso baseado em função (RBAC) do SnapCenter e as permissões ONTAP permitem que os administradores do SnapCenter deleguem o controle dos recursos do SnapCenter a diferentes usuários ou grupos de usuários. Esse acesso gerenciado centralmente permite que os administradores de aplicativos trabalhem com segurança em ambientes delegados.

Você pode criar e modificar funções e adicionar acesso a recursos aos usuários a qualquer momento. No entanto, ao configurar o SnapCenter pela primeira vez, você deve pelo menos adicionar usuários ou grupos do Active Directory às funções e, em seguida, adicionar acesso a recursos a esses usuários ou grupos.

Você não pode usar o SnapCenter para criar contas de usuário ou grupo. Você deve criar contas de usuário ou grupo no Active Directory do sistema operacional ou banco de dados.

Tipos de RBAC no SnapCenter

O SnapCenter usa os seguintes tipos de controle de acesso baseado em função:

- SnapCenter RBAC
- RBAC de nível de aplicação
- Plug-in SnapCenter para VMware vSphere RBAC
- Permissões da ONTAP

SnapCenter RBAC

O SnapCenter tem funções predefinidas e você pode atribuir usuários ou grupos de usuários a essas funções. As funções predefinidas são:

- Função de administrador do SnapCenter
- Função de administrador de backup e clonagem de aplicativos
- Função de Visualizador de Backup e Clone
- Função de administrador de infraestrutura

Quando você atribui uma função a um usuário, somente os trabalhos relevantes para esse usuário ficam visíveis na página Trabalhos, a menos que você tenha atribuído a função SnapCenterAdmin.

Você também pode criar novas funções e gerenciar permissões e usuários. Você pode atribuir permissões a usuários ou grupos para acessar objetos do SnapCenter , como hosts, conexões de armazenamento e grupos de recursos.

Você pode atribuir permissões RBAC a usuários e grupos dentro da mesma floresta e a usuários pertencentes a florestas diferentes. Não é possível atribuir permissões RBAC a usuários pertencentes a grupos aninhados em florestas.

Se você criar uma função personalizada, ela deverá conter todas as permissões da função SnapCenterAdmin. Se você copiar apenas algumas das permissões, por exemplo, Adicionar Host ou Remover Host, não poderá executar essas operações.

Os usuários precisam fornecer autenticação durante o login, por meio da interface gráfica do usuário (GUI) ou usando cmdlets do PowerShell. Se os usuários forem membros de mais de uma função, após inserir as credenciais de login, eles serão solicitados a especificar a função que desejam usar. Os usuários também precisam fornecer autenticação para executar as APIs.

RBAC de nível de aplicação

O SnapCenter usa credenciais para verificar se os usuários autorizados do SnapCenter também têm permissões no nível do aplicativo.

Por exemplo, se você quiser executar operações de proteção de dados em um ambiente SQL Server, deverá definir credenciais com as credenciais adequadas do Windows ou SQL. O SnapCenter Server autentica o conjunto de credenciais usando qualquer um dos métodos. Se você quiser executar operações de proteção de dados em um ambiente de sistema de arquivos do Windows no armazenamento ONTAP , a função de administrador do SnapCenter deverá ter privilégios de administrador no host do Windows.

Da mesma forma, se você quiser executar operações de proteção de dados em um banco de dados Oracle e se a autenticação do sistema operacional (SO) estiver desabilitada no host do banco de dados, você deverá definir credenciais com as credenciais do banco de dados Oracle ou do Oracle ASM. O SnapCenter Server autentica o conjunto de credenciais usando um destes métodos, dependendo da operação.

SnapCenter Plug-in for VMware vSphere RBAC

Se você estiver usando o plug-in SnapCenter VMware para proteção de dados consistente com VM, o vCenter Server fornecerá um nível adicional de RBAC. O plug-in SnapCenter VMware oferece suporte ao vCenter Server RBAC e ao ONTAP RBAC. "Saber mais"

Melhores práticas: a NetApp recomenda que você crie uma função ONTAP para as operações do SnapCenter Plug-in for VMware vSphere e atribua a ela todos os privilégios necessários.

Permissões da ONTAP

Você deve criar uma conta vsadmin com as permissões necessárias para acessar o sistema de armazenamento."Saber mais"

Permissões atribuídas às funções predefinidas do SnapCenter

Ao adicionar um usuário a uma função, você deve atribuir a permissão StorageConnection para habilitar a comunicação da máquina virtual de armazenamento (SVM) ou atribuir uma SVM ao usuário para habilitar a permissão de uso da SVM. A permissão Conexão de armazenamento permite que os usuários criem conexões SVM.

Por exemplo, um usuário com a função de administrador do SnapCenter pode criar conexões SVM e atribuí-las a um usuário com a função de administrador de backup e clonagem de aplicativos, que por padrão não tem permissão para criar ou editar conexões SVM. Sem uma conexão SVM, os usuários não podem concluir nenhuma operação de backup, clonagem ou restauração.

Função de administrador do SnapCenter

A função de administrador do SnapCenter tem todas as permissões habilitadas. Você não pode modificar as permissões para esta função. Você pode adicionar usuários e grupos à função ou removê-los.

Função de administrador de backup e clonagem de aplicativos

A função de administrador de backup e clonagem de aplicativos tem as permissões necessárias para executar ações administrativas para backups de aplicativos e tarefas relacionadas à clonagem. Esta função não tem permissões para gerenciamento de host, provisionamento, gerenciamento de conexão de armazenamento ou instalação remota.

Permissões	Habilitado	Criar	Ler	Atualizar	Excluir
Grupo de Recursos	Não aplicável	Sim	Sim	Sim	Sim
Política	Não aplicável	Sim	Sim	Sim	Sim
Backup	Não aplicável	Sim	Sim	Sim	Sim
Hospedar	Não aplicável	Sim	Sim	Sim	Sim
Conexão de armazenamento	Não aplicável	Não	Sim	Não	Não
Clone	Não aplicável	Sim	Sim	Sim	Sim
Provisão	Não aplicável	Não	Sim	Não	Não
Painel	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Relatórios	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restaurar	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Recurso	Sim	Sim	Sim	Sim	Sim
Instalação/Desinstalação de Plug-in	Não	Não aplicável		Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Monte	Sim	Sim	Não aplicável	Não aplicável	Não aplicável
Desmontar	Sim	Sim	Não aplicável	Não aplicável	Não aplicável
Restauração de volume total	Não	Não	Não aplicável	Não aplicável	Não aplicável
Proteção Secundária	Não	Não	Não aplicável	Não aplicável	Não aplicável

Permissões	Habilitado	Criar	Ler	Atualizar	Excluir
Monitor de tarefas	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Função de Visualizador de Backup e Clone

A função Visualizador de Backup e Clone tem visualização somente leitura de todas as permissões. Essa função também tem permissões habilitadas para descoberta, relatórios e acesso ao Painel.

Permissões	Habilitado	Criar	Ler	Atualizar	Excluir
Grupo de Recursos	Não aplicável	Não	Sim	Não	Não
Política	Não aplicável	Não	Sim	Não	Não
Backup	Não aplicável	Não	Sim	Não	Não
Hospedar	Não aplicável	Não	Sim	Não	Não
Conexão de armazenamento	Não aplicável	Não	Sim	Não	Não
Clone	Não aplicável	Não	Sim	Não	Não
Provisão	Não aplicável	Não	Sim	Não	Não
Painel	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Relatórios	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restaurar	Não	Não	Não aplicável	Não aplicável	Não aplicável
Recurso	Não	Não	Sim	Sim	Não
Instalação/Desinstalação de Plug-in	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Monte	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Desmontar	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Permissões	Habilitado	Criar	Ler	Atualizar	Excluir
Restauração de volume total	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Proteção Secundária	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Monitor de tarefas	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Função de administrador de infraestrutura

A função Administrador de Infraestrutura tem permissões habilitadas para gerenciamento de host, gerenciamento de armazenamento, provisionamento, grupos de recursos, relatórios de instalação remota e acesso ao Painel.

Permissões	Habilitado	Criar	Ler	Atualizar	Excluir
Grupo de Recursos	Não aplicável	Sim	Sim	Sim	Sim
Política	Não aplicável	Não	Sim	Sim	Sim
Backup	Não aplicável	Sim	Sim	Sim	Sim
Hospedar	Não aplicável	Sim	Sim	Sim	Sim
Conexão de armazenamento	Não aplicável	Sim	Sim	Sim	Sim
Clone	Não aplicável	Não	Sim	Não	Não
Provisão	Não aplicável	Sim	Sim	Sim	Sim
Painel	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Relatórios	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restaurar	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Recurso	Sim	Sim	Sim	Sim	Sim
Instalação/Desinstalação de Plug-in	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Permissões	Habilitado	Criar	Ler	Atualizar	Excluir
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Monte	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Desmontar	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restauração de volume total	Não	Não	Não aplicável	Não aplicável	Não aplicável
Proteção Secundária	Não	Não	Não aplicável	Não aplicável	Não aplicável
Monitor de tarefas	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Recuperação de desastres no SnapCenter

O recurso de recuperação de desastres (DR) do SnapCenter permite que você se recupere de desastres como corrupção de recursos ou falhas no servidor. Ele ajuda a restaurar o repositório SnapCenter , agendamentos do servidor, componentes de configuração e o plug-in SnapCenter para SQL Server e seu armazenamento.

Esta seção explica os dois tipos de DR no SnapCenter:

SnapCenter Server DR

- Os dados do SnapCenter Server são copiados e podem ser recuperados sem nenhum plug-in adicionado ou gerenciado pelo SnapCenter Server.
- O SnapCenter Server secundário deve ser instalado no mesmo diretório de instalação e na mesma porta que o SnapCenter Server primário.
- Para autenticação multifator (MFA), durante o SnapCenter Server DR, feche todas as guias do navegador e reabra um navegador para efetuar login novamente. Isso limpará os cookies de sessão existentes ou ativos e atualizará os dados de configuração corretos.
- A funcionalidade de recuperação de desastres do SnapCenter usa APIs REST para fazer backup do SnapCenter Server. Ver "Fluxos de trabalho da API REST para recuperação de desastres do SnapCenter Server" .
- O arquivo de configuração relacionado às configurações de auditoria não é feito backup no backup de DR e nem no servidor de DR após a operação de restauração. Você deve repetir manualmente as configurações do log de auditoria.

Plug-in SnapCenter e DR de armazenamento

O DR está disponível somente para o SnapCenter Plug-in para SQL Server. Se o plug-in estiver inativo, mude para outro host SQL e recupere os dados seguindo algumas etapas. Ver "Recuperação de desastres do plug-in SnapCenter para SQL Server" .

O SnapCenter usa o ONTAP SnapMirror para replicar dados, que podem ser usados para DR mantendo os dados sincronizados em um site secundário. Para iniciar o failover, interrompa a replicação do SnapMirror . Durante o fallback, inverta a sincronização para replicar dados do site de DR de volta para o local principal.

Licenças exigidas pelo SnapCenter

O SnapCenter requer várias licenças para habilitar a proteção de dados de aplicativos, bancos de dados, sistemas de arquivos e máquinas virtuais. O tipo de licença do SnapCenter que você instala depende do seu ambiente de armazenamento e dos recursos que você deseja usar.

Licença	Onde necessário
Controlador SnapCenter Standard baseado em	Obrigatório para FAS, AFF, ASA A licença SnapCenter Standard é uma licença baseada em controlador e está incluída como parte do NetApp ONTAP One. Se você tiver a licença do SnapManager Suite, também receberá o direito à licença do SnapCenter Standard. Se você quiser instalar o SnapCenter em caráter de teste com armazenamento FAS, AFF ou ASA , poderá obter uma licença de avaliação do NetApp ONTAP One entrando em contato com o representante de vendas. Para obter informações sobre licenças incluídas no NetApp ONTAP One, consulte "Licenças incluídas no NetApp ONTAP One" . O SnapCenter também é oferecido como parte do pacote de proteção de dados. Se você adquiriu o A400 ou posterior, deverá adquirir o pacote de proteção de dados.
SnapMirror ou SnapVault	ONTAP A licença SnapMirror ou SnapVault é necessária se a replicação estiver habilitada no SnapCenter.
SnapRestore	Necessário para restaurar e verificar backups. Em sistemas de armazenamento primário • Necessário em sistemas de destino SnapVault para executar verificação remota e restaurar a partir de um backup. • Obrigatório em sistemas de destino SnapMirror para executar verificação remota.

Licença	Onde necessário
FlexClone	Necessário para clonar bancos de dados e operações de verificação. Em sistemas de armazenamento primário e secundário • Obrigatório em sistemas de destino SnapVault para criar clones do backup do vault secundário. • Necessário em sistemas de destino SnapMirror para criar clones do backup secundário do SnapMirror .
Licenças de protocolo	• Licença iSCSI ou FC para LUNs • Licença CIFS para ações SMB • Licença NFS para VMDKs do tipo NFS • Licença iSCSI ou FC para VMDKs do tipo VMFS Obrigatório em sistemas de destino SnapMirror para fornecer dados se um volume de origem não estiver disponível.
Licenças SnapCenter Standard (opcional)	Destinos secundários ⓘ É recomendado, mas não obrigatório, que você adicione licenças do SnapCenter Standard a destinos secundários. Se as licenças do SnapCenter Standard não estiverem habilitadas em destinos secundários, você não poderá usar o SnapCenter para fazer backup de recursos no destino secundário após executar uma operação de failover. No entanto, uma licença FlexClone é necessária em destinos secundários para executar operações de clonagem e verificação.

Licença	Onde necessário
Licenças de recuperação de caixa de correio única (SMBR)	Se você estiver usando o SnapCenter Plug-in para Exchange para gerenciar bancos de dados do Microsoft Exchange Server e o Single Mailbox Recovery (SMBR), precisará de uma licença adicional para o SMBR, que precisa ser adquirida separadamente com base na caixa de correio do usuário. O NetApp® Single Mailbox Recovery chegou ao fim da disponibilidade (EOA) em 12 de maio de 2023. Para mais informações, consulte"CPC-00507" . A NetApp continuará a oferecer suporte aos clientes que adquiriram capacidade de caixa de correio, manutenção e suporte por meio de números de peça de marketing introduzidos em 24 de junho de 2020, durante a vigência do direito ao suporte. O NetApp Single Mailbox Recovery é um produto parceiro fornecido pela Ontrack. O Ontrack PowerControls oferece recursos semelhantes aos do NetApp Single Mailbox Recovery. Os clientes podem adquirir novas licenças de software Ontrack PowerControls e renovações de manutenção e suporte do Ontrack PowerControls da Ontrack (por meio de licensingteam@ontrack.com) para recuperação granular de caixa de correio após a data de EOA de 12 de maio de 2023.

As licenças SnapCenter Advanced e SnapCenter NAS File Services estão obsoletas e não estão mais disponíveis. A licença padrão e a licença baseada em capacidade não são mais necessárias para Amazon FSx for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP e Azure NetApp Files.

Você deve instalar uma ou mais licenças do SnapCenter . Para obter informações sobre como adicionar licenças, consulte"Adicionar licenças baseadas no controlador SnapCenter Standard" .

Sincronização ativa do SnapMirror no SnapCenter

A sincronização ativa do SnapMirror permite que os serviços empresariais continuem operando mesmo durante uma falha completa do site, permitindo que os aplicativos façam failover de forma transparente usando uma cópia secundária. Não é necessária intervenção manual nem script adicional para acionar um failover com a sincronização ativa do SnapMirror .

Para obter mais informações sobre a sincronização ativa do SnapMirror , consulte "Visão geral da sincronização ativa do SnapMirror" .

Para sincronização ativa do SnapMirror , certifique-se de ter atendido aos diversos requisitos de hardware, software e configuração do sistema. Para obter informações, consulte "Pré-requisitos"

Os plug-ins suportados para esse recurso são SnapCenter Plug-in para SQL Server, SnapCenter Plug-in para Windows, SnapCenter Plug-in para banco de dados Oracle, SnapCenter Plug-in para banco de dados SAP HANA, SnapCenter Plug-in para Microsoft Exchange Server e SnapCenter Plug-in para Unix.

Para oferecer suporte à proximidade do iniciador do host no SnapCenter, seu valor, origem ou destino, deve ser definido no ONTAP.

Os casos de uso não suportados no SnapCenter:

- Se você converter as cargas de trabalho de sincronização ativa assimétricas existentes do SnapMirror em simétricas alterando a política nos relacionamentos de sincronização ativa do SnapMirror de *automatedfailover* para *automatedfailoverduplex* no ONTAP, o mesmo não será suportado no SnapCenter.
- Se houver backups de um grupo de recursos (já protegido no SnapCenter) e a política de armazenamento for alterada nos relacionamentos de sincronização ativos do SnapMirror de *automatedfailover* para *automatedfailoverduplex* no ONTAP, o mesmo não será suportado no SnapCenter.

Conceitos-chave de proteção de dados

Antes de usar o SnapCenter, entenda os principais conceitos de backup, clonagem e restauração.

Recursos

Os recursos incluem bancos de dados, sistemas de arquivos do Windows ou compartilhamentos de arquivos copiados ou clonados com o SnapCenter. Dependendo do seu ambiente, os recursos também podem ser instâncias de banco de dados, grupos de disponibilidade do SQL Server, bancos de dados Oracle, bancos de dados RAC ou grupos de aplicativos personalizados.

Grupo de recursos

Um grupo de recursos é uma coleção de recursos em um host ou cluster, potencialmente de vários hosts e clusters. As operações executadas em um grupo de recursos se aplicam a todos os seus recursos com base no cronograma especificado. Você pode executar backups sob demanda ou agendados para recursos individuais ou grupos.

Se um host em um grupo de recursos compartilhados entrar no modo de manutenção, todas as operações agendadas para esse grupo serão suspensas em todos os hosts.

Use plug-ins relevantes para fazer backup de recursos específicos: plug-ins de banco de dados para bancos de dados, plug-ins de sistema de arquivos para sistemas de arquivos e SnapCenter Plug-in for VMware vSphere para VMs e datastores.

Políticas

As políticas especificam a frequência de backup, retenção de cópias, replicação, scripts e outras características das operações de proteção de dados.

Uma ou mais políticas podem ser selecionadas ao criar um grupo de recursos ou ao executar um backup sob demanda.

Um grupo de recursos define o que precisa ser protegido e quando deve ser protegido em termos de dia e hora. Uma política descreve como a proteção será realizada. Por exemplo, se for necessário fazer backup de todos os bancos de dados ou sistemas de arquivos de um host, um grupo de recursos incluindo todos os

bancos de dados ou sistemas de arquivos no host poderá ser criado. Duas políticas podem então ser anexadas ao grupo de recursos: uma política diária e uma política horária.

Ao criar o grupo de recursos e anexar as políticas, é possível configurá-lo para executar um backup completo diariamente e outro agendamento para backups de log a cada hora.

Prescrições e pós-escritos personalizados podem ser usados em operações de proteção de dados. Esses scripts permitem a automação antes ou depois do trabalho de proteção de dados. Por exemplo, um script pode notificar automaticamente sobre falhas ou avisos de tarefas de proteção de dados. Entender os requisitos para criar esses scripts é crucial antes de configurar prescrições e pós-escritos.

Uso de prescrições e posfácios

Prescrições e pós-escritos personalizados podem automatizar suas tarefas de proteção de dados antes ou depois do trabalho. Por exemplo, você pode adicionar um script para notificá-lo sobre falhas de trabalho ou avisos. Antes de configurá-los, certifique-se de entender os requisitos desses scripts.

Tipos de script suportados

Os seguintes tipos de scripts são suportados pelo Windows:

- Arquivos em lote
- Scripts do PowerShell
- Scripts Perl

Os seguintes tipos de scripts são suportados pelo UNIX:

- Scripts Perl
- Scripts Python
- Scripts de shell

> Junto com o shell bash padrão, outros shells como sh-shell, k-shell e c-shell também são suportados.

Caminho do script

Todos os prescrições e pós-escritos executados como parte das operações do SnapCenter em sistemas de armazenamento virtualizados e não virtualizados são executados no host do plug-in.

- Os scripts do Windows devem estar localizados no host do plug-in.

> O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_PATH.

- Os scripts UNIX devem estar localizados no host do plug-in.

> O caminho do script é validado no momento da execução.

Onde especificar scripts

Os scripts são especificados em políticas de backup. Quando uma tarefa de backup é iniciada, a política

associa automaticamente o script aos recursos que estão sendo copiados. Ao criar uma política de backup, você pode especificar os argumentos prescript e postscript.

Você não pode especificar vários scripts.

Tempo limite de script

O tempo limite é definido como 60 segundos, por padrão. Você pode modificar o valor do tempo limite.

Saída do script

O diretório padrão para os arquivos de saída de prescrições e postscripts do Windows é Windows\System32.

Não há um local padrão para os prescrições e pós-escritos do UNIX. Você pode redirecionar o arquivo de saída para qualquer local preferido.

Sistemas de armazenamento e aplicativos suportados pelo SnapCenter

Você deve conhecer os sistemas de armazenamento, aplicativos e bancos de dados suportados pelo SnapCenter.

Sistemas de armazenamento suportados

- NetApp ONTAP 9.12.1 e posterior
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

  Suporta memória não volátil expressa (NVMe) via Protocolo de Controle de Transporte (TCP).

  Para obter informações sobre o Amazon FSx for NetApp ONTAP, consulte "Documentação do Amazon FSx for NetApp ONTAP" .

- Sistemas NetApp ASA r2 que executam o NetApp ONTAP 9.16.1.

Aplicativos e bancos de dados suportados

O SnapCenter oferece suporte à proteção de diferentes aplicativos e bancos de dados. Para obter informações detalhadas sobre os aplicativos e bancos de dados suportados, consulte "Ferramenta de Matriz de Interoperabilidade da NetApp" .

O SnapCenter oferece suporte à proteção de cargas de trabalho Oracle e Microsoft SQL em ambientes de Software-Defined Data Center (SDDC) do VMware Cloud on Amazon Web Services (AWS). "Saber mais" .

Métodos de autenticação para credenciais do SnapCenter

As credenciais usam métodos de autenticação diferentes dependendo do aplicativo ou ambiente. As credenciais autenticam os usuários para que eles possam executar operações do SnapCenter . Você deve criar um conjunto de credenciais para instalar plug-ins e outro para operações de proteção de dados.

Autenticação do Windows

O método de autenticação do Windows autentica no Active Directory. Para autenticação do Windows, o Active Directory é configurado fora do SnapCenter. O SnapCenter autentica sem nenhuma configuração adicional. Você precisa de uma credencial do Windows para adicionar hosts, instalar pacotes de plug-ins e agendar tarefas.

Autenticação de domínio não confiável

O SnapCenter permite que usuários e grupos pertencentes a domínios não confiáveis criem credenciais do Windows. Para que a autenticação seja bem-sucedida, você deve registrar os domínios não confiáveis no SnapCenter.

Autenticação de grupo de trabalho local

O SnapCenter permite a criação de credenciais do Windows com usuários e grupos de grupos de trabalho locais. A autenticação do Windows para usuários e grupos de grupos de trabalho locais não ocorre durante a criação de credenciais do Windows, mas é adiada até que o registro do host e outras operações do host sejam executadas.

Autenticação do SQL Server

O método de autenticação SQL autentica em uma instância do SQL Server. Isso significa que uma instância do SQL Server deve ser descoberta no SnapCenter. Portanto, antes de adicionar uma credencial SQL, você deve adicionar um host, instalar pacotes de plug-in e atualizar os recursos. Você precisa da autenticação do SQL Server para executar operações como agendamento no SQL Server ou descobrir recursos.

Autenticação Linux

O método de autenticação do Linux autentica em um host Linux. Você precisa de autenticação do Linux durante a etapa inicial de adição do host Linux e instalação remota do Pacote de plug-ins do SnapCenter para Linux a partir da GUI do SnapCenter .

Autenticação AIX

O método de autenticação AIX autentica em um host AIX. Você precisa da autenticação do AIX durante a etapa inicial de adição do host do AIX e instalação remota do Pacote de plug-ins do SnapCenter para AIX a partir da GUI do SnapCenter .

Autenticação de banco de dados Oracle

O método de autenticação do banco de dados Oracle autentica em um banco de dados Oracle. Você precisa de uma autenticação de banco de dados Oracle para executar operações no banco de dados Oracle se a autenticação do sistema operacional (SO) estiver desabilitada no host do banco de dados. Portanto, antes de adicionar uma credencial de banco de dados Oracle, você deve criar um usuário Oracle no banco de dados Oracle com privilégios sysdba.

Autenticação Oracle ASM

O método de autenticação Oracle ASM autentica em uma instância do Oracle Automatic Storage Management (ASM). A autenticação do Oracle ASM será necessária se você precisar acessar uma instância do Oracle ASM e a autenticação do sistema operacional estiver desabilitada no host do banco de dados. Antes de adicionar uma credencial do Oracle ASM, crie um usuário Oracle com privilégios de sistema na instância do ASM.

Autenticação de catálogo RMAN

O método de autenticação do catálogo RMAN autentica no banco de dados do catálogo Oracle Recovery Manager (RMAN). Se você configurou um mecanismo de catálogo externo e registrou seu banco de dados no banco de dados de catálogo, será necessário adicionar a autenticação de catálogo do RMAN.

Operações SnapCenter suportadas para sistemas ASA r2

Os sistemas de armazenamento ASA r2 são suportados a partir do SnapCenter 6.1. "Saiba mais sobre os sistemas ASA r2"

O SnapCenter utiliza APIs REST para executar todas as operações em sistemas ASA r2, que não oferecem suporte a ZAPIs.

Operações suportadas pelo SnapCenter para sistemas ASA r2

- Criação de backups primários de aplicativos no VMDK
- Transferindo snapshots de grupo de consistência para sistema de armazenamento secundário
- Restaurar os backups dos sistemas de armazenamento primário e secundário para o host original ou para o host alternativo
  - Restauração no local de sistemas de armazenamento primário e secundário usando VMware vMotion
  - Conecte e copie e restaure dos sistemas de armazenamento primário e secundário
- Clonar os backups para o host original ou para o host alternativo

O SnapCenter pode descobrir ou criar grupos de consistência ONTAP . Ele também pode provisionar e inicializar relacionamentos SnapMirror com o cluster de destino para proteção secundária.

Para obter informações sobre como habilitar a proteção secundária em sistemas ASA r2 para seu aplicativo, consulte:

- "Habilitar proteção secundária para recursos do Microsoft SQL Server"
- "Habilitar proteção secundária para recursos do SAP HANA"
- "Habilitar proteção secundária para recursos Oracle"
- "Habilitar proteção secundária para sistemas de arquivos do Windows"
- "Habilitar proteção secundária para recursos do IBM Db2"
- "Habilitar proteção secundária para recursos do PostgreSQL"
- "Habilitar proteção secundária para recursos MySQL"
- "Habilitar proteção secundária para sistemas de arquivos Unix"

Operações não suportadas pelo SnapCenter para sistemas ASA r2

- Mapeamento de Dispositivos Brutos (RDM)
- Volumes de aplicativos para Oracle
- SAP HANA NDV
- LockVault
- Instantâneos à prova de violação

- Volumes FlexGroup
- Grupo de consistência hierárquica
- Migração de sistemas de armazenamento ASA, AFF ou FAS para sistemas de armazenamento ASA r2
- Proteção de bancos de dados que possuem uma mistura de recursos ASA, AFF ou FAS e recursos ASA r2
- Renomeação de snapshots
- Provisionamento secundário do diretório de log do host do plug-in SQL

Início rápido para o SnapCenter software

O guia de início rápido descreve as etapas básicas para instalar e configurar o SnapCenter software.

Preparar para instalar o SnapCenter Server

Você deve garantir que todos os requisitos para instalar o SnapCenter Server sejam atendidos.

- "Requisitos"
- "Registre-se para acessar o SnapCenter software"
- "Habilitar autenticação multifator"

Instalar o SnapCenter Server

O SnapCenter Server pode ser instalado em hosts Windows ou Linux. Baixe o pacote de instalação do SnapCenter Server em "Site de suporte da NetApp" e execute o instalador.

- "Instalar o servidor SnapCenter no Windows"
- "Instalar o SnapCenter Server no Linux"

Configurar o SnapCenter Server

Depois de instalar o SnapCenter Server, você deve configurá-lo com base no seu ambiente.

Instale o plug-in para seu aplicativo

Certifique-se de que todos os requisitos para instalar o plug-in específico do aplicativo sejam atendidos com base no aplicativo em uso e, em seguida, prossiga com a instalação do respectivo plug-in.

Proteja sua aplicação

Após instalar com sucesso o SnapCenter Server e os plug-ins necessários, você pode iniciar a criação de backups de aplicativos. Esses backups podem ser utilizados posteriormente para fins de restauração e clonagem, quando necessário.

Instalar e configurar o SnapCenter Server

Prepare-se para instalar o SnapCenter Server

Requisitos para instalar o SnapCenter Server

Antes de instalar o SnapCenter Server em um host Windows ou Linux, você deve revisar e garantir que todos os requisitos sejam atendidos para seu ambiente.

Requisitos de domínio e grupo de trabalho para host Windows

O SnapCenter Server pode ser instalado em um host Windows que esteja em um domínio ou em um grupo de trabalho.

O usuário com privilégios de administrador tem permissão para instalar o servidor SnapCenter .

- Domínio do Active Directory: você deve usar um usuário de domínio com direitos de administrador local. O usuário do domínio deve ser membro do grupo Administrador local no host Windows.
- Grupos de trabalho: você deve usar uma conta local que tenha direitos de administrador local.

Embora relações de confiança de domínio, florestas multidomínio e relações de confiança entre domínios sejam suportadas, domínios entre florestas não são suportados. A documentação da Microsoft sobre domínios e relações de confiança do Active Directory contém mais informações.

Após instalar o SnapCenter Server, você não deve alterar o domínio no qual o host SnapCenter está localizado. Se você remover o host do SnapCenter Server do domínio em que ele estava quando o SnapCenter Server foi instalado e tentar desinstalar o SnapCenter Server, a operação de desinstalação falhará.

Requisitos de espaço e dimensionamento

Você deve estar familiarizado com os requisitos de espaço e dimensionamento.

Item	Requisitos do host do Windows	Requisitos do host Linux
Sistemas Operacionais	Microsoft Windows Somente as versões em inglês, alemão, japonês e chinês simplificado dos sistemas operacionais são suportadas. Para obter as informações mais recentes sobre as versões suportadas, consultehttps://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT["Ferramenta de Matriz de Interoperabilidade da NetApp"^] .	• Red Hat Enterprise Linux (RHEL) 8 e 9 • Servidor SUSE Linux Enterprise (SLES) 15 Para obter as informações mais recentes sobre as versões suportadas, consultehttps://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT["Ferramenta de Matriz de Interoperabilidade da NetApp"^] .

Item	Requisitos do host do Windows	Requisitos do host Linux
Contagem mínima de CPU	4 núcleos	4 núcleos
RAM mínima	8 GB O pool de buffer do servidor MySQL usa 20% da RAM total.	8 GB
Espaço mínimo no disco rígido para o software e logs do SnapCenter Server	7 GB Se você tiver o repositório SnapCenter na mesma unidade onde o SnapCenter Server está instalado, é recomendável ter 15 GB.	15 GB
Espaço mínimo no disco rígido para o repositório SnapCenter	8 GB OBSERVAÇÃO: se você tiver o SnapCenter Server na mesma unidade onde o repositório do SnapCenter está instalado, é recomendável ter 15 GB.	Não aplicável

Item	Requisitos do host do Windows	Requisitos do host Linux
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell 7.4.2 ou posterior Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet" .	• .NET Framework 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell 7.4.2 ou posterior • Nginx é um servidor web que pode ser usado como um proxy reverso • Pam-devel PAM (Pluggable Authentication Modules) é uma ferramenta de segurança do sistema que permite que os administradores de sistema definam políticas de autenticação sem precisar recompilar programas que fazem autenticação.

O ASP.NET Core precisa do IIS_IUSRS para acessar o sistema de arquivos temporário no SnapCenter Server no Windows.

Requisitos do host SAN

O SnapCenter não inclui utilitários de host ou um DSM. Se o host SnapCenter fizer parte de um ambiente SAN (FC/iSCSI), talvez seja necessário instalar e configurar software adicional no host do SnapCenter Server.

- Utilitários de host: Os utilitários de host oferecem suporte a FC e iSCSI e permitem que você use MPIO em seus servidores Windows. "Saber mais" .
- Microsoft DSM para Windows MPIO: Este software funciona com drivers Windows MPIO para gerenciar vários caminhos entre computadores host NetApp e Windows. Um DSM é necessário para configurações de alta disponibilidade.

Se você estava usando o ONTAP DSM, você deve migrar para o Microsoft DSM. Para obter mais informações, consulte "Como migrar do ONTAP DSM para o Microsoft DSM" .

Requisitos do navegador

O SnapCenter software é compatível com o Chrome 125 e posteriores e o Microsoft Edge 110.0.1587.17 e posteriores.

Requisitos portuários

O SnapCenter software requer portas diferentes para comunicação entre diferentes componentes.

- Os aplicativos não podem compartilhar uma porta.
- Para portas personalizáveis, você pode selecionar uma porta personalizada durante a instalação se não quiser usar a porta padrão.

- Para portas fixas, você deve aceitar o número de porta padrão.
- Firewalls
  - Firewalls, proxies ou outros dispositivos de rede não devem interferir nas conexões.
  - Se você especificar uma porta personalizada ao instalar o SnapCenter, deverá adicionar uma regra de firewall no host do plug-in para essa porta para o SnapCenter Plug-in Loader.

A tabela a seguir lista as diferentes portas e seus valores padrão.

Nome da porta	Números de porta	Protocolo	Direção	Descrição
Porta SnapCenter	8146	HTTPS	Bidirecional	Esta porta é usada para comunicação entre o cliente SnapCenter (o usuário SnapCenter) e o SnapCenter Server e também é usada para comunicação dos hosts de plug-in com o SnapCenter Server. Você pode personalizar o número da porta.
Porta de comunicação SnapCenter SMCore	8145	HTTPS	Bidirecional	Esta porta é usada para comunicação entre o SnapCenter Server e os hosts onde os plug-ins do SnapCenter estão instalados. Você pode personalizar o número da porta.

Nome da porta	Números de porta	Protocolo	Direção	Descrição
Porta de serviço do agendador	8154	HTTPS		Esta porta é usada para orquestrar os fluxos de trabalho do agendador do SnapCenter para todos os plug-ins gerenciados no host do servidor SnapCenter de maneira centralizada. Você pode personalizar o número da porta.
Porta RabbitMQ	5672	TCP		Esta é a porta padrão na qual o RabbitMQ escuta e é usada para comunicação do modelo publicador-assinante entre o serviço Scheduler e o SnapCenter.
Porta MySQL	3306	HTTPS		A porta é usada para comunicação com o banco de dados do repositório SnapCenter . Você pode criar conexões seguras do SnapCenter Server para o servidor MySQL."Saber mais"
Hosts de plug-ins do Windows	135, 445	TCP		Esta porta é usada para comunicação entre o SnapCenter Server e o host no qual o plug-in está sendo instalado. O intervalo de portas dinâmicas adicionais especificado pela Microsoft também deve ser aberto.

Nome da porta	Números de porta	Protocolo	Direção	Descrição
Hosts de plug-in Linux ou AIX	22	SSH	Unidirecional	Esta porta é usada para comunicação entre o SnapCenter Server e o host, iniciada do servidor para o host cliente.
Pacote de plug-ins SnapCenter para Windows, Linux ou AIX	8145	HTTPS	Bidirecional	Esta porta é usada para comunicação entre o SMCore e os hosts onde o pacote de plug-ins está instalado. Personalizável. Você pode personalizar o número da porta.
Plug-in SnapCenter para banco de dados Oracle	27216			A porta JDBC padrão é usada pelo plug-in para Oracle para conexão ao banco de dados Oracle.
Plug-in SnapCenter para banco de dados Exchange	909			A porta NET.TCP padrão é usada pelo plug-in para Windows para conexão aos retornos de chamada do Exchange VSS.
Plug-ins compatíveis com a NetApp para SnapCenter	9090	HTTPS		Esta é uma porta interna usada somente no host do plug-in; nenhuma exceção de firewall é necessária. A comunicação entre o SnapCenter Server e os plug-ins é roteada pela porta 8145.

Nome da porta	Números de porta	Protocolo	Direção	Descrição
Cluster ONTAP ou porta de comunicação SVM	• 443 (HTTPS) • 80 (HTTP)	• HTTPS • HTTP	Bidirecional	A porta é usada pelo SAL (Storage Abstraction Layer) para comunicação entre o host que executa o SnapCenter Server e o SVM. Atualmente, a porta também é usada pelo SAL nos hosts do plug-in SnapCenter for Windows para comunicação entre o host do plug-in SnapCenter e o SVM.
Plug-in SnapCenter para banco de dados SAP HANA	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	Bidirecional	Para um contêiner de banco de dados multilocatário (MDC) de locatário único, o número da porta termina em 13; para um não MDC, o número da porta termina em 15. Você pode personalizar o número da porta.
Plug-in SnapCenter para PostgreSQL	5432			Esta porta é a porta padrão do PostgreSQL usada para comunicação do plug-in do PostgreSQL com o cluster do PostgreSQL. Você pode personalizar o número da porta.

Registre-se para acessar o SnapCenter software

Você deve se registrar para acessar o SnapCenter software se for novo no Amazon FSx for NetApp ONTAP ou Azure NetApp Files e não tiver uma conta NetApp existente.

Antes de começar

- Você deve ter acesso ao ID de e-mail corporativo.
- Se você estiver usando o Azure NetApp Files, deverá ter o ID de assinatura do Azure.
- Se estiver usando o Amazon FSx for NetApp ONTAP, você deverá ter o ID do sistema de arquivos do seu sistema de arquivos FSx para ONTAP .

Sobre esta tarefa

Seu registro está sujeito a validações de informações e pode levar até um dia para confirmar e atualizar a nova conta do NetApp Support Site (NSS) para acesso **total** a partir do acesso **de convidado**.

Passos

1. Clique https://mysupport.netapp.com/site/user/registration para registro.
2. Insira seu ID de e-mail corporativo, preencha o captcha, aceite a política de privacidade da NetApp e clique em **Enviar**.
3. Autentique o registro inserindo o OTP enviado para seu ID de e-mail e clique em **Continuar**.
4. Na página de conclusão do registro, insira os seguintes detalhes para concluir o registro.
   a. Selecione * Cliente NetApp / Usuário final*.
   b. No campo NÚMERO DE SÉRIE, insira a ID da assinatura do Azure se estiver usando o Azure NetApp Files ou a ID do sistema de arquivos se estiver usando o Amazon FSx for NetApp ONTAP.

Você pode abrir um tíquete em https://mysupport.netapp.com/site/help se você enfrentar algum problema durante o registro ou para saber o status.

Autenticação multifator (MFA)

Gerenciar autenticação multifator (MFA)

Você pode gerenciar a funcionalidade de autenticação multifator (MFA) no servidor do Serviço de Federação do Active Directory (AD FS) e no SnapCenter Server.

Habilitar autenticação multifator (MFA)

Você pode habilitar a funcionalidade MFA para o SnapCenter Server usando comandos do PowerShell.

Sobre esta tarefa

- O SnapCenter oferece suporte a logins baseados em SSO quando outros aplicativos são configurados no mesmo AD FS. Em determinadas configurações do AD FS, o SnapCenter pode exigir autenticação do usuário por motivos de segurança, dependendo da persistência da sessão do AD FS.
- As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando `Get-Help command_name` . Alternativamente, você também pode ver "Guia de referência do cmdlet do software SnapCenter" .

Antes de começar

- O Serviço de Federação do Active Directory (AD FS) do Windows deve estar ativo e em execução no respectivo domínio.
- Você deve ter um serviço de autenticação multifator compatível com AD FS, como Azure MFA, Cisco Duo e assim por diante.

- O registro de data e hora do servidor SnapCenter e AD FS deve ser o mesmo, independentemente do fuso horário.
- Obtenha e configure o certificado de CA autorizado para o SnapCenter Server.

  O Certificado CA é obrigatório pelos seguintes motivos:

  - Garante que as comunicações ADFS-F5 não sejam interrompidas porque os certificados autoassinados são exclusivos no nível do nó.
  - Garante que durante a atualização, o reparo ou a recuperação de desastres (DR) em uma configuração autônoma ou de alta disponibilidade, o certificado autoassinado não seja recriado, evitando assim a reconfiguração do MFA.
  - Garante resoluções IP-FQDN.

    Para obter informações sobre o certificado CA, consulte"Gerar arquivo CSR de certificado CA" .

Passos

1. Conecte-se ao host dos Serviços de Federação do Active Directory (AD FS).
2. Baixe o arquivo de metadados da federação do AD FS em"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copie o arquivo baixado para o SnapCenter Server para habilitar o recurso MFA.
4. Efetue login no SnapCenter Server como usuário administrador do SnapCenter por meio do PowerShell.
5. Usando a sessão do PowerShell, gere o arquivo de metadados do SnapCenter MFA usando o cmdlet *New-SmMultifactorAuthenticationMetadata -path*.

   O parâmetro path especifica o caminho para salvar o arquivo de metadados MFA no host do SnapCenter Server.
6. Copie o arquivo gerado para o host do AD FS para configurar o SnapCenter como a entidade do cliente.
7. Habilite o MFA para o SnapCenter Server usando o `Set-SmMultiFactorAuthentication` cmdlet.
8. (Opcional) Verifique o status e as configurações da configuração do MFA usando `Get-SmMultiFactorAuthentication` cmdlet.
9. Acesse o console de gerenciamento da Microsoft (MMC) e execute as seguintes etapas:
   a. Clique em **Arquivo** > **Adicionar/Remover Snapin**.
   b. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
   c. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
   d. Clique em **Console Root** > **Certificados – Computador local** > **Pessoal** > **Certificados**.
   e. Clique com o botão direito do mouse no certificado CA vinculado ao SnapCenter e selecione **Todas as tarefas** > **Gerenciar chaves privadas**.
   f. No assistente de permissões, execute as seguintes etapas:
      i. Clique em **Adicionar**.
      ii. Clique em **Locais** e selecione o host em questão (topo da hierarquia).
      iii. Clique em **OK** na janela pop-up **Locais**.
      iv. No campo de nome do objeto, digite 'IIS_IUSRS', clique em **Verificar nomes** e clique em **OK**.

Se a verificação for bem-sucedida, clique em **OK**.

10. No host do AD FS, abra o assistente de gerenciamento do AD FS e execute as seguintes etapas:
    a. Clique com o botão direito em **Relying Party Trusts** > **Adicionar Relying Party Trust** > **Iniciar**.
    b. Selecione a segunda opção, navegue pelo arquivo de metadados do SnapCenter MFA e clique em **Avançar**.
    c. Especifique um nome de exibição e clique em **Avançar**.
    d. Escolha uma política de controle de acesso conforme necessário e clique em **Avançar**.
    e. Selecione as configurações na próxima aba como padrão.
    f. Clique em **Concluir**.

    O SnapCenter agora é refletido como uma parte confiável com o nome de exibição fornecido.

11. Selecione o nome e execute os seguintes passos:
    a. Clique em **Editar política de emissão de reivindicações**.
    b. Clique em **Adicionar regra** e clique em **Avançar**.
    c. Especifique um nome para a regra de reivindicação.
    d. Selecione **Active Directory** como o armazenamento de atributos.
    e. Selecione o atributo como **User-Principal-Name** e o tipo de declaração de saída como **Name-ID**.
    f. Clique em **Concluir**.
12. Execute os seguintes comandos do PowerShell no servidor ADFS.

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

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

13. Execute as seguintes etapas para confirmar se os metadados foram importados com sucesso.
    a. Clique com o botão direito do mouse na parte confiável e selecione **Propriedades**.
    b. Certifique-se de que os campos Endpoints, Identificadores e Assinatura estejam preenchidos.
14. Feche todas as abas do navegador e abra-o novamente para limpar os cookies de sessão existentes ou ativos e faça login novamente.

A funcionalidade SnapCenter MFA também pode ser habilitada usando APIs REST.

Para obter informações sobre solução de problemas, consulte "Tentativas simultâneas de login em várias guias mostram erro de MFA" .

Atualizar metadados do AD FS MFA

Você deve atualizar os metadados do AD FS MFA no SnapCenter sempre que houver qualquer modificação no servidor AD FS, como atualização, renovação de certificado CA, DR e assim por diante.

Passos

1. Baixe o arquivo de metadados da federação do AD FS em"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"

2. Copie o arquivo baixado para o SnapCenter Server para atualizar a configuração do MFA.
3. Atualize os metadados do AD FS no SnapCenter executando o seguinte cmdlet:

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

4. Feche todas as abas do navegador e abra-o novamente para limpar os cookies de sessão existentes ou ativos e faça login novamente.

Atualizar metadados do SnapCenter MFA

Você deve atualizar os metadados do SnapCenter MFA no AD FS sempre que houver qualquer modificação no servidor ADFS, como reparo, renovação de certificado CA, DR e assim por diante.

Passos

1. No host do AD FS, abra o assistente de gerenciamento do AD FS e execute as seguintes etapas:
   a. Selecione **Relying Party Trusts**.
   b. Clique com o botão direito do mouse na parte confiável que foi criada para o SnapCenter e selecione **Excluir**.

      O nome definido pelo usuário da parte confiável será exibido.

   c. Habilite a autenticação multifator (MFA).

      Ver "Habilitar autenticação multifator" .
2. Feche todas as abas do navegador e abra-o novamente para limpar os cookies de sessão existentes ou ativos e faça login novamente.

Desativar autenticação multifator (MFA)

Passos

1. Desabilite o MFA e limpe os arquivos de configuração que foram criados quando o MFA foi habilitado usando o `Set-SmMultiFactorAuthentication` cmdlet.
2. Feche todas as abas do navegador e abra-o novamente para limpar os cookies de sessão existentes ou ativos e faça login novamente.

Gerenciar autenticação multifator (MFA) usando Rest API, PowerShell e SCCLI

O login MFA é compatível com navegador, API REST, PowerShell e SCCLI. O MFA é suportado por um gerenciador de identidade do AD FS. Você pode habilitar o MFA, desabilitar o MFA e configurar o MFA a partir da GUI, API REST, PowerShell e SCCLI.

Configurar o AD FS como OAuth/OIDC

Configurar o AD FS usando o assistente da GUI do Windows

1. Navegue até **Painel do Gerenciador de Servidores** > **Ferramentas** > **Gerenciamento do ADFS**.
2. Navegue até **ADFS** > **Grupos de Aplicativos**.
   a. Clique com o botão direito do mouse em **Grupos de aplicativos**.
   b. Selecione **Adicionar grupo de aplicativos** e insira **Nome do aplicativo**.

c. Selecione **Aplicativo do Servidor**.

d. Clique em **Avançar**.

3. Copie **Identificador do Cliente**.

   Este é o ID do cliente. .. Adicione URL de retorno de chamada (URL do SnapCenter Server) na URL de redirecionamento. .. Clique em **Avançar**.

4. Selecione **Gerar segredo compartilhado**.

   Copie o valor secreto. Este é o segredo do cliente. .. Clique em **Avançar**.

5. Na página **Resumo**, clique em **Avançar**.

   a. Na página **Concluído**, clique em **Fechar**.

6. Clique com o botão direito do mouse no **Grupo de Aplicativos** recém-adicionado e selecione **Propriedades**.

7. Selecione **Adicionar aplicativo** em Propriedades do aplicativo.

8. Clique em **Adicionar aplicativo**.

   Selecione Web API e clique em **Avançar**.

9. Na página Configurar API da Web, insira a URL do SnapCenter Server e o Identificador do Cliente criados na etapa anterior na seção Identificador.

   a. Clique em **Adicionar**.

   b. Clique em **Avançar**.

10. Na página **Escolher política de controle de acesso**, selecione a política de controle com base em suas necessidades (por exemplo, Permitir todos e exigir MFA) e clique em **Avançar**.

11. Na página **Configurar permissão do aplicativo**, por padrão o openid é selecionado como um escopo, clique em **Avançar**.

12. Na página **Resumo**, clique em **Avançar**.

    Na página **Concluído**, clique em **Fechar**.

13. Na página **Propriedades do aplicativo de exemplo**, clique em **OK**.

14. Token JWT emitido por um servidor de autorização (AD FS) e destinado a ser consumido pelo recurso.

    A declaração 'aud' ou de público deste token deve corresponder ao identificador do recurso ou da API da Web.

15. Edite a WebAPI selecionada e verifique se o URL de retorno de chamada (URL do SnapCenter Server) e o identificador do cliente foram adicionados corretamente.

    Configure o OpenID Connect para fornecer um nome de usuário como declarações.

16. Abra a ferramenta **Gerenciamento do AD FS** localizada no menu **Ferramentas** no canto superior direito do Gerenciador do Servidor.

    a. Selecione a pasta **Grupos de Aplicativos** na barra lateral esquerda.

    b. Selecione a API da Web e clique em **EDITAR**.

    c. Guia de regras de transformação de emissão

17. Clique em **Adicionar regra**.
    a. Selecione **Enviar atributos LDAP como declarações** no menu suspenso Modelo de regra de declaração.
    b. Clique em **Avançar**.
18. Digite o nome da **Regra de reivindicação**.
    a. Selecione **Active Directory** no menu suspenso Armazenamento de atributos.
    b. Selecione **Nome-Principal-do-Usuário** no menu suspenso **Atributo LDAP** e **UPN** no menu suspenso Tipo de Reivindicação de Saída*.
    c. Clique em **Concluir**.

Criar grupo de aplicativos usando comandos do PowerShell

Você pode criar o grupo de aplicativos, a API da Web e adicionar o escopo e as declarações usando comandos do PowerShell. Esses comandos estão disponíveis em formato de script automatizado. Para mais informações, consulte <link para o artigo da KB>.

1. Crie o novo Grupo de Aplicativos no AD FS usando o seguinte comando.

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

   `ClientRoleIdentifier`nome do seu grupo de aplicação

   `redirectURL`URL válida para redirecionamento após autorização

2. Crie o aplicativo do servidor AD FS e gere o segredo do cliente.

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

3. Crie o aplicativo ADFS Web API e configure o nome da política que ele deve usar.

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

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

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

4. Obtenha o ID do cliente e o segredo do cliente da saída dos comandos a seguir, pois eles são exibidos apenas uma vez.

   ```
   "client_id = $identifier"

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

5. Conceda ao aplicativo AD FS as permissões allatclaims e openid.

   ```
   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. Escreva o arquivo de regras de transformação.

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

7. Nomeie o aplicativo Web API e defina suas regras de transformação de emissão usando um arquivo externo.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Atualizar tempo de expiração do token de acesso

Você pode atualizar o tempo de expiração do token de acesso usando o comando do PowerShell.

Sobre esta tarefa

- Um token de acesso pode ser usado somente para uma combinação específica de usuário, cliente e recurso. Os tokens de acesso não podem ser revogados e são válidos até expirarem.
- Por padrão, o tempo de expiração de um token de acesso é de 60 minutos. Este tempo mínimo de expiração é suficiente e dimensionado. Você deve fornecer valor suficiente para evitar quaisquer trabalhos críticos para os negócios em andamento.

Etapa

Para atualizar o tempo de expiração do token de acesso para um grupo de aplicativos WebApi, use o seguinte comando no servidor AD FS.

+

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

Obter o token do portador do AD FS

Você deve preencher os parâmetros mencionados abaixo em qualquer cliente REST (como o Postman) e ele solicitará que você preencha as credenciais do usuário. Além disso, você deve inserir a autenticação de segundo fator (algo que você tem e algo que você é) para obter o token do portador.

+ A validade do token portador é configurável no servidor AD FS por aplicativo e o período de validade padrão é de 60 minutos.

Campo	Valor
Tipo de subsídio	Código de autorização
URL de retorno de chamada	Insira a URL base do seu aplicativo se você não tiver uma URL de retorno de chamada.
URL de autenticação	[adfs-nome-de-domínio]/adfs/oauth2/autorizar
URL do token de acesso	[nome-de-domínio-adfs]/adfs/oauth2/token
ID do cliente	Insira o ID do cliente do AD FS
Segredo do cliente	Digite o segredo do cliente do AD FS
Escopo	OpenID
Autenticação do cliente	Enviar como cabeçalho AUTH básico
Recurso	Na aba **Opções Avançadas**, adicione o campo Recurso com o mesmo valor que o URL de retorno de chamada, que vem como um valor “aud” no token JWT.

Configurar MFA no SnapCenter Server usando PowerShell, SCCLI e REST API

Você pode configurar o MFA no SnapCenter Server usando PowerShell, SCCLI e REST API.

Autenticação SnapCenter MFA CLI

No PowerShell e no SCCLI, o cmdlet existente (Open-SmConnection) é estendido com mais um campo chamado "AccessToken" para usar o token do portador para autenticar o usuário.

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

Após a execução do cmdlet acima, uma sessão é criada para o respectivo usuário executar outros cmdlets do SnapCenter .

Autenticação SnapCenter MFA Rest API

Use o token portador no formato *Authorization=Bearer <access token>* no cliente REST API (como Postman ou swagger) e mencione o RoleName do usuário no cabeçalho para obter uma resposta bem-sucedida do SnapCenter.

Fluxo de trabalho da API REST do MFA

Quando o MFA é configurado com o AD FS, você deve autenticar usando um token de acesso (portador) para acessar o aplicativo SnapCenter por qualquer API Rest.

Sobre esta tarefa

- Você pode usar qualquer cliente REST, como Postman, Swagger UI ou FireCamp.
- Obtenha um token de acesso e use-o para autenticar solicitações subsequentes (SnapCenter Rest API) para executar qualquer operação.

Passos

Para autenticar através do AD FS MFA

1. Configure o cliente REST para chamar o ponto de extremidade do AD FS para obter o token de acesso.

   Ao clicar no botão para obter um token de acesso para um aplicativo, você será redirecionado para a página SSO do AD FS, onde deverá fornecer suas credenciais do AD e autenticar com o MFA. 1. Na página SSO do AD FS, digite seu nome de usuário ou e-mail na caixa de texto Nome de usuário.

   + Os nomes de usuário devem ser formatados como usuário@domínio ou domínio\usuário.

2. Na caixa de texto Senha, digite sua senha.
3. Clique em **Entrar**.
4. Na seção **Opções de login**, selecione uma opção de autenticação e autentique (dependendo da sua configuração).
   - Push: aprove a notificação push que é enviada para seu telefone.
   - Código QR: Use o aplicativo móvel AUTH Point para escanear o código QR e digite o código de verificação mostrado no aplicativo
   - Senha de uso único: digite a senha de uso único para seu token.
5. Após a autenticação bem-sucedida, um pop-up será aberto contendo o acesso, o ID e o token de atualização.

   Copie o token de acesso e use-o na API Rest do SnapCenter para executar a operação.

6. Na API Rest, você deve passar o token de acesso e o nome da função na seção de cabeçalho.
7. O SnapCenter valida esse token de acesso do AD FS.

   Se for um token válido, o SnapCenter o decodifica e obtém o nome de usuário.

8. Usando o nome de usuário e o nome da função, o SnapCenter autentica o usuário para uma execução de API.

   Se a autenticação for bem-sucedida, o SnapCenter retornará o resultado, caso contrário, uma mensagem de erro será exibida.

Habilitar ou desabilitar a funcionalidade SnapCenter MFA para REST API, CLI e GUI

GUI

Passos

1. Efetue login no SnapCenter Server como Administrador do SnapCenter .
2. Clique em **Configurações** > **Configurações globais** > **Configurações de autenticação multifator (MFA)**
3. Selecione a interface (GUI/RST API/CLI) para habilitar ou desabilitar o login MFA.

Interface do PowerShell

Passos

1. Execute os comandos do PowerShell ou da CLI para habilitar o MFA para GUI, REST API, PowerShell e SCCLI.

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

   O parâmetro path especifica o local do arquivo XML de metadados do AD FS MFA.

   Habilita o MFA para SnapCenter GUI, Rest API, PowerShell e SCCLI configurados com o caminho de arquivo de metadados do AD FS especificado.

2. Verifique o status e as configurações da configuração do MFA usando o `Get-SmMultiFactorAuthentication` cmdlet.

Interface SCCLI

Passos

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

APIs REST

1. Execute a seguinte API de postagem para habilitar MFA para GUI, REST API, PowerShell e SCCLI.

Parâmetro	Valor
URL solicitada	/api/4.9/settings/autenticação multifator
Método HTTP	Publicar
Corpo da solicitação	{ "IsGuiMFAEnabled": falso, "IsRestApiMFAEnabled": verdadeiro, "IsCliMFAEnabled": falso, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" }

Corpo de Resposta	{ "MFAConfiguration": { "IsGuiMFAEnabled": falso, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": nulo, "IsRestApiMFAEnabled": verdadeiro, "IsCliMFAEnabled": falso, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

2. Verifique o status e as configurações da configuração do MFA usando a seguinte API.

Parâmetro	Valor
URL solicitada	/api/4.9/settings/autenticação multifator
Método HTTP	Pegar
Corpo de Resposta	{ "MFAConfiguration": { "IsGuiMFAEnabled": falso, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": nulo, "IsRestApiMFAEnabled": verdadeiro, "IsCliMFAEnabled": falso, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

Instalar o SnapCenter Server

Instalar o SnapCenter Server no host Windows

Você pode executar o executável do instalador do SnapCenter Server para instalar o SnapCenter Server.

Opcionalmente, você pode executar vários procedimentos de instalação e configuração usando cmdlets do PowerShell. Você deve usar o PowerShell 7.4.2 ou posterior.

A instalação silenciosa do SnapCenter Server a partir da linha de comando não é suportada.

Antes de começar

- O host do SnapCenter Server deve estar atualizado com as atualizações do Windows, sem reinicializações pendentes do sistema.
- Você deve ter certeza de que o MySQL Server não está instalado no host onde você planeja instalar o SnapCenter Server.
- Você deve ter habilitado a depuração do instalador do Windows.

  Consulte o site da Microsoft para obter informações sobre como habilitar "Registro do instalador do Windows" .

Você não deve instalar o SnapCenter Server em um host que tenha o Microsoft Exchange Server, o Active Directory ou servidores de nomes de domínio.

Passos

1. Baixe o pacote de instalação do SnapCenter Server em "Site de suporte da NetApp" .
2. Inicie a instalação do SnapCenter Server clicando duas vezes no arquivo .exe baixado.

   Após iniciar a instalação, todas as pré-verificações são executadas e, se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas são exibidas.

   Você pode ignorar as mensagens de aviso e prosseguir com a instalação; no entanto, os erros deverão ser corrigidos.

3. Revise os valores pré-preenchidos necessários para a instalação do SnapCenter Server e modifique-os, se necessário.

   Você não precisa especificar a senha para o banco de dados do repositório do MySQL Server. Durante a instalação do SnapCenter Server, a senha é gerada automaticamente.

   O caractere especial “%” is not supported in the custom path for the repository database. If you include "` %`" no caminho, a instalação falha.

4. Clique em **Instalar agora**.

   Se você tiver especificado algum valor inválido, mensagens de erro apropriadas serão exibidas. Você deve inserir novamente os valores e então iniciar a instalação.

   Se você clicar no botão **Cancelar**, a etapa que está sendo executada será concluída e, em seguida, iniciará a operação de reversão. O SnapCenter Server será completamente removido do host.

   Entretanto, se você clicar em **Cancelar** quando as operações "Reinicialização do site do SnapCenter Server" ou "Aguardando o início do SnapCenter Server" estiverem sendo executadas, a instalação prosseguirá sem cancelar a operação.

   Os arquivos de log são sempre listados (os mais antigos primeiro) na pasta %temp% do usuário administrador. Se você quiser redirecionar os locais de log, inicie a instalação do SnapCenter Server no prompt de comando executando:`C:\installer_location\installer_name.exe /log"C:\"`

Recursos habilitados no host Windows durante a instalação

O instalador do SnapCenter Server habilita os recursos e funções do Windows no seu host Windows durante a instalação. Elas podem ser interessantes para solução de problemas e manutenção do sistema host.

Categoria	Recurso
Servidor Web	• Serviços de Informação da Internet • Serviços da World Wide Web • Recursos HTTP comuns ◦ Documento Padrão ◦ Navegação de diretório ◦ Erros HTTP ◦ Redirecionamento HTTP ◦ Conteúdo estático ◦ Publicação WebDAV • Saúde e Diagnóstico ◦ Registro personalizado ◦ Registro HTTP ◦ Ferramentas de registro ◦ Monitor de Solicitação ◦ Rastreamento • Recursos de desempenho ◦ Compressão de conteúdo estático • Segurança ◦ Segurança IP ◦ Autenticação Básica ◦ Suporte centralizado para certificado SSL ◦ Autenticação de mapeamento de certificado de cliente ◦ Autenticação de mapeamento de certificado do cliente IIS ◦ Restrições de IP e domínio ◦ Filtragem de solicitações ◦ Autorização de URL ◦ Autenticação do Windows • Recursos de desenvolvimento de aplicativos ◦ Extensibilidade .NET 4.5 ◦ Inicialização do aplicativo ◦ Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) ◦ Inclusões do lado do servidor ◦ Protocolo WebSocket Ferramentas de Gestão Console de gerenciamento do IIS

Categoria	Recurso
Scripts e ferramentas de gerenciamento do IIS	• Serviço de Gerenciamento do IIS • Ferramentas de gerenciamento da Web
Recursos do .NET Framework 8.0.12	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • Ativação HTTP do Windows Communication Foundation (WCF)45 ◦ Ativação TCP ◦ Ativação HTTP Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet" .
Enfileiramento de mensagens	• Serviços de enfileiramento de mensagens Certifique-se de que nenhum outro aplicativo use o serviço MSMQ que o SnapCenter cria e gerencia. • RabbitMQ • Erlang
Serviço de Ativação de Processos do Windows	• Modelo de Processo
APIs de configuração	Todos

Instalar o SnapCenter Server no host Linux

Você pode executar o executável do instalador do SnapCenter Server para instalar o SnapCenter Server.

Antes de começar

- Se você quiser instalar o SnapCenter Server usando um usuário não root que não tenha privilégios suficientes para instalar o SnapCenter, obtenha o arquivo de soma de verificação sudoers no site de suporte da NetApp . Você deve usar o arquivo de soma de verificação apropriado com base na versão do Linux.
- Se o pacote sudo não estiver disponível no SUSE Linux, instale-o para evitar falhas de autenticação.
- Para o SUSE Linux, configure o nome do host para evitar falha na instalação.
- Verifique o status seguro do Linux executando o comando `sestatus` . Se o *status do SELinux* for "habilitado" e o *modo atual* for "imposto", execute o seguinte:
  - Execute o comando: `sudo semanage port -a -t http_port_t -p tcp`

`<WEBAPP_EXTERNAL_PORT_>`

O valor padrão de *WEBAPP_EXTERNAL_PORT* é 8146

- Se o firewall bloquear a porta, execute `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

  O valor padrão de *WEBAPP_EXTERNAL_PORT* é 8146

- Execute os seguintes comandos no diretório onde você tem permissão de leitura e gravação:
  - `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

    Se o comando retornar "nada a fazer", execute-o novamente após instalar o SnapCenter Server.

  - Se o comando criar *my-nginx.pp*, execute o comando para tornar o pacote de política ativo: `sudo semodule -i my-nginx.pp`
- O caminho usado para o diretório MySQL PID é */var/opt/mysqld*. Execute os seguintes comandos para definir as permissões para instalação do MySQL.
  - `mkdir /var/opt/mysqld`
  - `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`
  - `sudo restorecon -Rv /var/opt/mysqld`
- O caminho usado para o diretório de dados do MySQL é */INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/*. Execute os seguintes comandos para definir as permissões para o diretório de dados do MySQL.
  - `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`

Sobre esta tarefa

- Quando o SnapCenter Server é instalado no host Linux, serviços de terceiros, como MySQL, RabbitMq e Errlang, são instalados. Você não deve desinstalá-los.
- O SnapCenter Server instalado no host Linux não suporta:
  - Alta disponibilidade
  - Plug-ins do Windows
  - Active Directory (suporta apenas usuários locais, tanto usuários root quanto não root com credenciais)
  - Autenticação baseada em chave para efetuar login no SnapCenter
- Durante a instalação do .NET Runtime, se a instalação não resolver as dependências da biblioteca *libicu*, instale *libicu* executando o comando: `yum install -y libicu`
- Se a instalação do SnapCenter Server falhar devido à indisponibilidade do *Perl*, instale o *Perl* executando o comando: `yum install -y perl`

Passos

1. Baixe o seguinte de "Site de suporte da NetApp" para */diretório inicial*.

- Pacote de instalação do SnapCenter Server - **snapcenter-linux-server-(el8/el9/sles15).bin**
- Arquivo de chave pública - **snapcenter_public_key.pub**
- Arquivo de assinatura respectivo - **snapcenter-linux-server-(el8/el9/sles15).bin.sig**

2. Valide o arquivo de assinatura.
   `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. Para instalação de usuário não root, adicione o conteúdo visudo especificado em **snapcenter_server_checksum_(el8/el9/sles15).txt** disponível junto com o instalador .bin.
4. Atribua a permissão de execução para o instalador .bin.
   `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. Execute uma das ações para instalar o SnapCenter Server.

Se você quiser executar…	Faça isso…
Instalação interativa	`./snapcenter-linux-server-(el8/el9/sles15).bin` Você será solicitado a inserir os seguintes detalhes: • A porta externa do webapp usada para acessar o SnapCenter Server fora do host Linux. O valor padrão é 8146. • O usuário do SnapCenter Server que instalará o SnapCenter Server. • O diretório de instalação onde os pacotes serão instalados.

Se você quiser executar…	Faça isso…
Instalação não interativa	`sudo ./snapcenter-linux-server-(el8/el9/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>` Exemplo: sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOG_NAME=InstallerLog.log Os logs serão armazenados em */var/opt/snapcenter/logs*. Parâmetros a serem passados para instalar o SnapCenter Server: • DWEBAPP_EXTERNAL_PORT: Porta externa do Webapp usada para acessar o SnapCenter Server fora do host Linux. O valor padrão é 8146. • DWEBAPP_INTERNAL_PORT: Porta interna do Webapp usada para acessar o SnapCenter Server no host Linux. O valor padrão é 8147. • DSMCORE_PORT: Porta SMCore na qual os serviços smcore estão sendo executados. O valor padrão é 8145. • DSCHEDULER_PORT: Porta do agendador na qual os serviços do agendador estão sendo executados. O valor padrão é 8154. • DSNAPCENTER_SERVER_USER: Usuário do SnapCenter Server que instalará o SnapCenter Server. Para *DSNAPCENTER_SERVER_USER*, o padrão é o usuário que executa o instalador. • DUSER_INSTALL_DIR: Diretório de instalação onde os pacotes serão instalados. Para *DUSER_INSTALL_DIR*, o diretório de instalação padrão é */opt*. • DINSTALL_LOG_NAME: Nome do arquivo de log onde os logs de instalação serão armazenados. Este é um parâmetro opcional e, se especificado, nenhum log será exibido no console. Se você não especificar este parâmetro, os logs serão exibidos no console e também armazenados no arquivo de log padrão. DSELINUX: Se o *status do SELinux* for

O que vem a seguir?

- Se o *status do SELinux* for "habilitado" e o *modo atual* for "imposto", o serviço **nginx** falhará ao iniciar. Você deve executar os seguintes comandos:
  a. Vá para o diretório inicial.
  b. Execute o comando: `journalctl -x|grep nginx`
  c. Se a porta interna do Webapp (8147) não tiver permissão para escutar, execute os seguintes comandos:
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. Correr `setsebool -P httpd_can_network_connect on`

- "habilitado", o *modo atual* for "imposto" e você tiver executado os comandos mencionados na seção Antes de começar, especifique este parâmetro e atribua o valor como 1. O valor padrão é 0.
- DUPGRADE: O valor padrão é 0. Especifique este parâmetro e seu valor como qualquer número inteiro diferente de 0 para atualizar o SnapCenter Server.

Recursos habilitados no host Linux durante a instalação

O SnapCenter Server instala os pacotes de software abaixo que podem ajudar na solução de problemas e na manutenção do sistema host.

- Rabbitmq
- Erlang

Registrar SnapCenter

Se você é novo nos produtos NetApp e não tem uma conta NetApp existente, registre o SnapCenter para habilitar o suporte.

Passos

1. Após instalar o SnapCenter, navegue até **Ajuda > Sobre**.
2. Na caixa de diálogo *Sobre o SnapCenter*, anote a instância do SnapCenter , um número de 20 dígitos que começa com 971.
3. Clique https://register.netapp.com .
4. Clique em *Não sou um cliente registrado da NetApp *.
5. Especifique seus dados para se registrar.
6. Deixe o campo SN de referência da NetApp em branco.
7. Selecione * SnapCenter* no menu suspenso Linha de produtos.
8. Selecione o provedor de cobrança.
9. Insira o ID da instância do SnapCenter de 20 dígitos.
10. Clique em **Enviar**.

Efetue login no SnapCenter usando autorização RBAC

O SnapCenter oferece suporte ao controle de acesso baseado em função (RBAC). O administrador do SnapCenter atribui funções e recursos por meio do SnapCenter RBAC a um usuário no grupo de trabalho ou no Active Directory, ou a grupos no Active Directory. O usuário do RBAC agora pode fazer login no SnapCenter com as funções atribuídas.

Antes de começar

- Você deve habilitar o Serviço de Ativação de Processos do Windows (WAS) no Gerenciador do Windows Server.
- Se você quiser usar o Internet Explorer como navegador para efetuar login no SnapCenter Server, certifique-se de que o Modo Protegido no Internet Explorer esteja desabilitado.
- Se o SnapCenter Server estiver instalado no host Linux, você deverá efetuar login usando a conta de usuário que foi usada para instalar o SnapCenter Server.

Sobre esta tarefa

Durante a instalação, o assistente de instalação do SnapCenter Server cria um atalho e o coloca na área de trabalho e no menu Iniciar do host onde o SnapCenter está instalado. Além disso, no final da instalação, o assistente de instalação exibe o URL do SnapCenter com base nas informações fornecidas durante a instalação, que você pode copiar se quiser fazer login de um sistema remoto.

Se você tiver várias guias abertas no seu navegador, fechar apenas a guia do navegador SnapCenter não fará seu logout do SnapCenter. Para encerrar sua conexão com o SnapCenter, você deve sair do SnapCenter clicando no botão **Sair** ou fechando todo o navegador da web.

Melhores práticas: Por motivos de segurança, é recomendável que você não habilite seu navegador para salvar sua senha do SnapCenter .

A URL da GUI padrão é uma conexão segura com a porta padrão 8146 no servidor onde o SnapCenter Server está instalado (*https://server:8146*). Se você forneceu uma porta de servidor diferente durante a instalação do SnapCenter , essa porta será usada.

Para implantação de Alta Disponibilidade (HA), você deve acessar o SnapCenter usando o IP do cluster virtual *https://Virtual_Cluster_IP_or_FQDN:8146*. Se você não vir a interface do usuário do SnapCenter ao navegar até *https://Virtual_Cluster_IP_or_FQDN:8146* no Internet Explorer (IE), adicione o endereço IP ou FQDN do Virtual Cluster como um site confiável no IE em cada host de plug-in ou desative a Segurança Aprimorada do IE em cada host de plug-in. Para obter mais informações, consulte "Não é possível acessar o endereço IP do cluster de uma rede externa" .

Além de usar a GUI do SnapCenter , você pode usar cmdlets do PowerShell para criar scripts para executar operações de configuração, backup e restauração. Alguns cmdlets podem ter mudado a cada versão do SnapCenter . O "Guia de referência do cmdlet do software SnapCenter" tem os detalhes.

Se estiver efetuando login no SnapCenter pela primeira vez, você deverá fazer login usando as credenciais fornecidas durante o processo de instalação.

Passos

1. Inicie o SnapCenter a partir do atalho localizado na área de trabalho do host local, ou a partir da URL fornecida no final da instalação, ou a partir da URL fornecida pelo administrador do SnapCenter .
2. Insira as credenciais do usuário.

Para especificar o seguinte…	Use um destes formatos…
Administrador de domínio	• NetBIOS\Nome de usuário • Sufixo UserName@UPN Por exemplo, username@netapp.com • Domínio FQDN\Nome de usuário
Administrador local	Nome de usuário

3. Se você tiver mais de uma função atribuída, na caixa Função, selecione a função que deseja usar para esta sessão de login.

   Seu usuário atual e a função associada são exibidos no canto superior direito do SnapCenter depois que você faz login.

Resultado

A página Painel é exibida.

Se o registro falhar com o erro de que o site não pode ser acessado, você deve mapear o certificado SSL para o SnapCenter. "Saber mais"

Depois que você terminar

Após efetuar login no SnapCenter Server como um usuário RBAC pela primeira vez, atualize a lista de recursos.

Se você tiver domínios não confiáveis do Active Directory que deseja que o SnapCenter suporte, registre esses domínios no SnapCenter antes de configurar as funções para os usuários em domínios não confiáveis. "Saber mais" .

Se você quiser adicionar o host do plug-in no SnapCenter em execução no host Linux, deverá obter o arquivo de soma de verificação no local: */opt/ NetApp/snapcenter/SnapManagerWeb/Repository*.

A partir da versão 6.0, um atalho para o SnapCenter PowerShell é criado na área de trabalho. Você pode acessar diretamente os cmdlets do SnapCenter PowerShell usando o atalho.

Efetue login no SnapCenter usando a autenticação multifator (MFA)

O SnapCenter Server oferece suporte a MFA para contas de domínio, que fazem parte do diretório ativo.

Antes de começar

Você deveria ter habilitado o MFA. Para obter informações sobre como habilitar o MFA, consulte"Habilitar autenticação multifator"

Sobre esta tarefa

- Somente FQDN é suportado
- Usuários de grupos de trabalho e de domínio cruzado não podem efetuar login usando MFA

Passos

1. Inicie o SnapCenter a partir do atalho localizado na área de trabalho do host local, ou a partir da URL fornecida no final da instalação, ou a partir da URL fornecida pelo administrador do SnapCenter .
2. Na página de login do AD FS, insira o nome de usuário e a senha.

   Quando a mensagem de erro de nome de usuário ou senha inválidos for exibida na página do AD FS, você deve verificar o seguinte:

   - Se o nome de usuário ou a senha são válidos

     A conta de usuário deve existir no Active Directory (AD)

   - Se você excedeu o máximo de tentativas permitidas definido no AD
   - Se o AD e o AD FS estão ativos e em execução

Modificar o tempo limite da sessão da GUI padrão do SnapCenter

Você pode modificar o período de tempo limite da sessão da GUI do SnapCenter para torná-lo menor ou maior que o período de tempo limite padrão de 20 minutos.

Como recurso de segurança, após um período padrão de 15 minutos de inatividade, o SnapCenter avisa que você será desconectado da sessão da GUI em 5 minutos. Por padrão, o SnapCenter desconecta você da sessão da GUI após 20 minutos de inatividade, e você deve efetuar login novamente.

Passos

1. No painel de navegação esquerdo, clique em **Configurações** > **Configurações globais**.
2. Na página Configurações globais, clique em **Configurações de configuração**.
3. No campo Tempo limite da sessão, insira o novo tempo limite da sessão em minutos e clique em **Salvar**.

Proteja o servidor web SnapCenter desabilitando o SSL 3.0

Por motivos de segurança, você deve desabilitar o protocolo Secure Socket Layer (SSL) 3.0 no Microsoft IIS se ele estiver habilitado no seu servidor web SnapCenter .

Há falhas no protocolo SSL 3.0 que um invasor pode usar para causar falhas de conexão ou realizar ataques man-in-the-middle e observar o tráfego de criptografia entre seu site e seus visitantes.

Passos

1. Para iniciar o Editor do Registro no host do servidor web SnapCenter , clique em **Iniciar** > **Executar** e digite regedit.
2. No Editor do Registro, navegue até HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\.
   - Se a chave do servidor já existir:
     i. Selecione o DWORD habilitado e clique em **Editar** > **Modificar**.
     ii. Altere o valor para 0 e clique em **OK**.
   - Se a chave do servidor não existir:

i. Clique em **Editar** > **Novo** > **Chave** e nomeie a chave como Servidor.

ii. Com a nova chave do servidor selecionada, clique em **Editar** > **Novo** > **DWORD**.

iii. Nomeie o novo DWORD como Habilitado e insira 0 como valor.

3. Feche o Editor do Registro.

Configurar o SnapCenter Server

Adicionar e provisionar o sistema de armazenamento

Adicionar sistemas de armazenamento

Você deve configurar o sistema de armazenamento que dá ao SnapCenter acesso ao armazenamento ONTAP , aos sistemas ASA r2 ou ao Amazon FSx for NetApp ONTAP para executar operações de proteção e provisionamento de dados.

Você pode adicionar um SVM autônomo ou um cluster composto por vários SVMs. Se estiver usando o Amazon FSx for NetApp ONTAP, você pode adicionar o LIF de administração do FSx composto por vários SVMs usando a conta fsxadmin ou adicionar o FSx SVM no SnapCenter.

Antes de começar

- Você deve ter as permissões necessárias na função de administrador de infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estejam em andamento.

  As instalações do plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento porque o cache do host pode não ser atualizado e o status dos bancos de dados pode ser exibido na GUI do SnapCenter como “Não disponível para backup” ou "`Não no armazenamento NetApp ".

- Os nomes dos sistemas de armazenamento devem ser exclusivos.

  O SnapCenter não oferece suporte a vários sistemas de armazenamento com o mesmo nome em clusters diferentes. Cada sistema de armazenamento suportado pelo SnapCenter deve ter um nome exclusivo e um endereço IP LIF de dados exclusivo.

Sobre esta tarefa

- Ao configurar sistemas de armazenamento, você também pode habilitar os recursos do Sistema de Gerenciamento de Eventos (EMS) e do AutoSupport . A ferramenta AutoSupport coleta dados sobre a integridade do seu sistema e os envia automaticamente ao suporte técnico da NetApp , permitindo que eles solucionem problemas do seu sistema.

  Se você habilitar esses recursos, o SnapCenter enviará informações do AutoSupport ao sistema de armazenamento e mensagens EMS ao syslog do sistema de armazenamento quando um recurso for protegido, uma operação de restauração ou clonagem for concluída com sucesso ou uma operação falhar.

- Se você estiver planejando replicar Snapshots para um destino SnapMirror ou SnapVault , deverá configurar conexões do sistema de armazenamento para o SVM ou Cluster de destino, bem como para o SVM ou Cluster de origem.

Se você alterar a senha do sistema de armazenamento, os trabalhos agendados, o backup sob demanda e as operações de restauração poderão falhar. Depois de alterar a senha do sistema de armazenamento, você pode atualizá-la clicando em **Modificar** na guia Armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Sistemas de armazenamento**.
2. Na página Sistemas de Armazenamento, clique em **Novo**.
3. Na página Adicionar sistema de armazenamento, forneça as seguintes informações:

Para este campo…	Faça isso…
Sistema de armazenamento	Digite o nome do sistema de armazenamento ou endereço IP. Os nomes dos sistemas de armazenamento, sem incluir o nome de domínio, devem ter 15 caracteres ou menos e devem ser resolvíveis. Para criar conexões de sistema de armazenamento com nomes com mais de 15 caracteres, você pode usar o cmdlet Add-SmStorageConnectionPowerShell. Para sistemas de armazenamento com configuração MetroCluster (MCC), é recomendável registrar clusters locais e pares para operações sem interrupções. O SnapCenter não oferece suporte a várias SVMs com o mesmo nome em clusters diferentes. Cada SVM suportado pelo SnapCenter deve ter um nome exclusivo. Depois de adicionar a conexão de armazenamento ao SnapCenter, você não deve renomear o SVM ou o Cluster usando o ONTAP. Se o SVM for adicionado com um nome curto ou FQDN, ele deverá ser resolvível tanto no SnapCenter quanto no host do plug-in.
Nome de usuário/Senha	Insira as credenciais do usuário de armazenamento que tem os privilégios necessários para acessar o sistema de armazenamento.

Para este campo…	Faça isso…
Configurações do Sistema de Gerenciamento de Eventos (EMS) e AutoSupport	Se você quiser enviar mensagens EMS para o syslog do sistema de armazenamento ou se quiser que mensagens do AutoSupport sejam enviadas ao sistema de armazenamento para proteção aplicada, operações de restauração concluídas ou operações com falha, marque a caixa de seleção apropriada. Quando você seleciona a caixa de seleção **Enviar notificação do AutoSupport para operações com falha no sistema de armazenamento**, a caixa de seleção **Registrar eventos do SnapCenter Server no syslog** também é selecionada porque o sistema de mensagens EMS é necessário para habilitar as notificações do AutoSupport .

4. Clique em **Mais opções** se quiser modificar os valores padrão atribuídos à plataforma, protocolo, porta e tempo limite.

   a. Em Plataforma, selecione uma das opções na lista suspensa.

      Se o SVM for o sistema de armazenamento secundário em um relacionamento de backup, marque a caixa de seleção **Secundário**. Quando a opção **Secundária** é selecionada, o SnapCenter não executa uma verificação de licença imediatamente.

   Se você adicionou SVM no SnapCenter , o usuário precisa selecionar manualmente o tipo de plataforma no menu suspenso.

   a. Em Protocolo, selecione o protocolo que foi configurado durante a configuração do SVM ou do Cluster, normalmente HTTPS.
   b. Digite a porta que o sistema de armazenamento aceita.

      A porta padrão 443 normalmente funciona.

   c. Insira o tempo em segundos que deve decorrer antes que as tentativas de comunicação sejam interrompidas.

      O valor padrão é 60 segundos.

   d. Se o SVM tiver várias interfaces de gerenciamento, marque a caixa de seleção **IP preferencial** e insira o endereço IP preferencial para conexões SVM.
   e. Clique em **Salvar**.
5. Clique em **Enviar**.

Resultado

Na página Sistemas de Armazenamento, no menu suspenso **Tipo**, execute uma das seguintes ações:

- Selecione * ONTAP SVMs * se quiser visualizar todos os SVMs que foram adicionados.

  Se você adicionou FSx SVMs, eles serão listados aqui.

- Selecione * Clusters ONTAP * se quiser visualizar todos os clusters que foram adicionados.

  Se você adicionou clusters FSx usando fsxadmin, os clusters FSx serão listados aqui.

  Ao clicar no nome do cluster, todas as SVMs que fazem parte do cluster são exibidas na seção Máquinas Virtuais de Armazenamento.

  Se um novo SVM for adicionado ao cluster ONTAP usando a GUI do ONTAP , clique em **Rediscover** para visualizar o SVM recém-adicionado.

Depois que você terminar

Um administrador de cluster deve habilitar o AutoSupport em cada nó do sistema de armazenamento para enviar notificações por e-mail de todos os sistemas de armazenamento aos quais o SnapCenter tem acesso, executando o seguinte comando na linha de comando do sistema de armazenamento:

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

O administrador da Máquina Virtual de Armazenamento (SVM) não tem acesso ao AutoSupport.

Conexões e credenciais de armazenamento

Antes de executar operações de proteção de dados, você deve configurar as conexões de armazenamento e adicionar as credenciais que o SnapCenter Server e os plug-ins do SnapCenter usarão.

Conexões de armazenamento

As conexões de armazenamento dão ao SnapCenter Server e aos plug-ins do SnapCenter acesso ao armazenamento ONTAP . A configuração dessas conexões também envolve a configuração dos recursos do AutoSupport e do Sistema de Gerenciamento de Eventos (EMS).

Credenciais

- Administrador de domínio ou qualquer membro do grupo de administradores

  Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são:

  - *NetBIOS\Nome do Usuário*
  - *FQDN do domínio\Nome do usuário*
  - *Nome de usuário@upn*
- Administrador local (somente para grupos de trabalho)

  Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host.

  O formato válido para o campo Nome de usuário é: *UserName*

- Credenciais para grupos de recursos individuais

  Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver privilégios de administrador completos, será necessário atribuir pelo menos os privilégios de grupo de recursos e backup ao nome de usuário.

Provisionar armazenamento em hosts Windows

Criar e gerenciar igroups

Crie grupos de iniciadores (igroups) para especificar quais hosts podem acessar um determinado LUN no sistema de armazenamento. Você pode usar o SnapCenter para criar, renomear, modificar ou excluir um igroup em um host Windows.

Criar um igroup

Você pode usar o SnapCenter para criar um igroup em um host Windows. O igroup estará disponível no assistente Criar Disco ou Conectar Disco quando você mapear o igroup para um LUN.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Igroup**.
3. Na página Grupos de Iniciadores, clique em **Novo**.
4. Na caixa de diálogo Criar Igroup, defina o igroup:

Neste campo…	Faça isso…
Sistema de armazenamento	Selecione o SVM para o LUN que você mapeará para o igroup.
Hospedar	Selecione o host no qual você deseja criar o igroup.
Nome do Igroup	Digite o nome do igroup.
Iniciadores	Selecione o iniciador.
Tipo	Selecione o tipo de iniciador, iSCSI, FCP ou misto (FCP e iSCSI).

5. Quando estiver satisfeito com suas entradas, clique em **OK**.

   O SnapCenter cria o igroup no sistema de armazenamento.

Renomear um igroup

Você pode usar o SnapCenter para renomear um igroup existente.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Igroup**.
3. Na página Grupos de Iniciadores, clique no campo **Máquina Virtual de Armazenamento** para exibir uma lista de SVMs disponíveis e, em seguida, selecione a SVM para o igroup que você deseja renomear.
4. Na lista de igroups do SVM, selecione o igroup que deseja renomear e clique em **Renomear**.
5. Na caixa de diálogo Renomear igroup, insira o novo nome para o igroup e clique em **Renomear**.

Modificar um igroup

Você pode usar o SnapCenter para adicionar iniciadores de igroup a um igroup existente. Ao criar um igroup, você pode adicionar apenas um host. Se você quiser criar um igroup para um cluster, poderá modificar o igroup para adicionar outros nós a esse igroup.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Igroup**.
3. Na página Grupos de Iniciadores, clique no campo **Máquina Virtual de Armazenamento** para exibir uma lista suspensa de SVMs disponíveis e selecione a SVM para o igroup que você deseja modificar.
4. Na lista de igroups, selecione um igroup e clique em **Adicionar iniciador ao igroup**.
5. Selecione um host.
6. Selecione os iniciadores e clique em **OK**.

Excluir um igroup

Você pode usar o SnapCenter para excluir um igroup quando não precisar mais dele.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Igroup**.
3. Na página Grupos de Iniciadores, clique no campo **Máquina Virtual de Armazenamento** para exibir uma lista suspensa de SVMs disponíveis e selecione a SVM para o igroup que você deseja excluir.
4. Na lista de igroups do SVM, selecione o igroup que deseja excluir e clique em **Excluir**.
5. Na caixa de diálogo Excluir igroup, clique em **OK**.

   O SnapCenter exclui o igroup.

Criar e gerenciar discos

O host do Windows vê LUNs no seu sistema de armazenamento como discos virtuais. Você pode usar o SnapCenter para criar e configurar um LUN conectado via FC ou via iSCSI.

- O SnapCenter suporta apenas discos básicos. Os discos dinâmicos não são suportados.
- Para GPT, apenas uma partição de dados é permitida e para MBR, uma partição primária com um volume formatado com NTFS ou CSVFS e um caminho de montagem.

- Estilos de partição suportados: GPT, MBR; em uma VM VMware UEFI, apenas discos iSCSI são suportados

> O SnapCenter não suporta renomear um disco. Se um disco gerenciado pelo SnapCenter for renomeado, as operações do SnapCenter não serão bem-sucedidas.

Visualizar os discos em um host

Você pode visualizar os discos em cada host Windows que você gerencia com o SnapCenter.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o host na lista suspensa **Host**.

   Os discos estão listados.

Exibir discos agrupados

Você pode visualizar discos clusterizados no cluster que você gerencia com o SnapCenter. Os discos em cluster são exibidos somente quando você seleciona o cluster no menu suspenso Hosts.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o cluster na lista suspensa **Host**.

   Os discos estão listados.

Estabelecer uma sessão iSCSI

Se estiver usando iSCSI para se conectar a um LUN, você deverá estabelecer uma sessão iSCSI antes de criar o LUN para habilitar a comunicação.

Antes de começar

- Você deve ter definido o nó do sistema de armazenamento como um destino iSCSI.
- Você deve ter iniciado o serviço iSCSI no sistema de armazenamento. "Saber mais"

Sobre esta tarefa

Você pode estabelecer uma sessão iSCSI somente entre as mesmas versões de IP, de IPv6 para IPv6 ou de IPv4 para IPv4.

Você pode usar um endereço IPv6 de link local para gerenciamento de sessão iSCSI e para comunicação entre um host e um destino somente quando ambos estiverem na mesma sub-rede.

Se você alterar o nome de um iniciador iSCSI, o acesso aos destinos iSCSI será afetado. Após alterar o nome, talvez seja necessário reconfigurar os destinos acessados pelo iniciador para que eles possam

reconhecer o novo nome. Você deve reiniciar o host após alterar o nome de um iniciador iSCSI.

Se o seu host tiver mais de uma interface iSCSI, depois de estabelecer uma sessão iSCSI com o SnapCenter usando um endereço IP na primeira interface, você não poderá estabelecer uma sessão iSCSI de outra interface com um endereço IP diferente.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Sessão iSCSI**.
3. Na lista suspensa **Máquina Virtual de Armazenamento**, selecione a máquina virtual de armazenamento (SVM) para o destino iSCSI.
4. Na lista suspensa **Host**, selecione o host da sessão.
5. Clique em **Estabelecer Sessão**.

   O assistente Estabelecer Sessão é exibido.

6. No assistente Estabelecer Sessão, identifique o destino:

Neste campo…	Digitar…
Nome do nó de destino	O nome do nó do destino iSCSI Se houver um nome de nó de destino existente, o nome será exibido em formato somente leitura.
Endereço do portal de destino	O endereço IP do portal da rede de destino
Porta do portal de destino	A porta TCP do portal da rede de destino
Endereço do portal do iniciador	O endereço IP do portal da rede iniciadora

7. Quando estiver satisfeito com suas entradas, clique em **Conectar**.

   O SnapCenter estabelece a sessão iSCSI.

8. Repita este procedimento para estabelecer uma sessão para cada alvo.

Crie LUNs ou discos conectados por FC ou iSCSI

O host do Windows vê os LUNs no seu sistema de armazenamento como discos virtuais. Você pode usar o SnapCenter para criar e configurar um LUN conectado via FC ou via iSCSI.

Se você quiser criar e formatar discos fora do SnapCenter, somente os sistemas de arquivos NTFS e CSVFS são suportados.

Antes de começar

- Você deve ter criado um volume para o LUN no seu sistema de armazenamento.

  O volume deve conter apenas LUNs e apenas LUNs criados com o SnapCenter.

Não é possível criar um LUN em um volume clone criado SnapCenter, a menos que o clone já tenha sido dividido.

- Você deve ter iniciado o serviço FC ou iSCSI no sistema de armazenamento.
- Se estiver usando iSCSI, você deverá ter estabelecido uma sessão iSCSI com o sistema de armazenamento.
- O pacote de plug-ins do SnapCenter para Windows deve ser instalado somente no host no qual você está criando o disco.

Sobre esta tarefa

- Não é possível conectar um LUN a mais de um host, a menos que o LUN seja compartilhado por hosts em um cluster de failover do Windows Server.
- Se um LUN for compartilhado por hosts em um cluster de failover do Windows Server que usa CSV (Cluster Shared Volumes), você deverá criar o disco no host que possui o grupo de clusters.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o host na lista suspensa **Host**.
4. Clique em **Novo**.

   O assistente Criar disco é aberto.

5. Na página Nome do LUN, identifique o LUN:

Neste campo…	Faça isso…
Sistema de armazenamento	Selecione o SVM para o LUN.
Caminho LUN	Clique em **Procurar** para selecionar o caminho completo da pasta que contém o LUN.
Nome da LUN	Digite o nome do LUN.
Tamanho do cluster	Selecione o tamanho de alocação do bloco LUN para o cluster. O tamanho do cluster depende do sistema operacional e dos aplicativos.
Rótulo LUN	Opcionalmente, insira um texto descritivo para o LUN.

6. Na página Tipo de disco, selecione o tipo de disco:

Selecione…	Se…
Disco dedicado	O LUN pode ser acessado por apenas um host. Ignore o campo **Grupo de recursos**.
Disco compartilhado	O LUN é compartilhado por hosts em um cluster de failover do Windows Server. Insira o nome do grupo de recursos do cluster no campo **Grupo de recursos**. Você precisa criar o disco em apenas um host no cluster de failover.
Volume compartilhado do cluster (CSV)	O LUN é compartilhado por hosts em um cluster de failover do Windows Server que usa CSV. Insira o nome do grupo de recursos do cluster no campo **Grupo de recursos**. Certifique-se de que o host no qual você está criando o disco seja o proprietário do grupo de clusters.

7. Na página Propriedades da unidade, especifique as propriedades da unidade:

Propriedade	Descrição
Atribuição automática de ponto de montagem	O SnapCenter atribui automaticamente um ponto de montagem de volume com base na unidade do sistema. Por exemplo, se a unidade do sistema for C:, a atribuição automática criará um ponto de montagem de volume na unidade C: (C:\scmnpt\). A atribuição automática não é suportada para discos compartilhados.
Atribuir letra de unidade	Monte o disco na unidade selecionada na lista suspensa adjacente.
Usar ponto de montagem de volume	Monte o disco no caminho da unidade especificado no campo adjacente. A raiz do ponto de montagem do volume deve pertencer ao host no qual você está criando o disco.
Não atribua letra de unidade ou ponto de montagem de volume	Escolha esta opção se preferir montar o disco manualmente no Windows.
Tamanho da LUN	Especifique o tamanho do LUN; mínimo de 150 MB. Selecione MB, GB ou TB na lista suspensa ao lado.

Propriedade	Descrição
Use o provisionamento fino para o volume que hospeda este LUN	Provisionamento fino do LUN. O provisionamento fino aloca apenas a quantidade de espaço de armazenamento necessária de cada vez, permitindo que o LUN cresça eficientemente até a capacidade máxima disponível. Certifique-se de que haja espaço suficiente disponível no volume para acomodar todo o armazenamento LUN que você acha que precisará.
Escolha o tipo de partição	Selecione a partição GPT para uma tabela de partição GUID ou a partição MBR para um registro mestre de inicialização. Partições MBR podem causar problemas de desalinhamento em clusters de failover do Windows Server. Discos de partição de interface de firmware extensível unificada (UEFI) não são suportados.

8. Na página Map LUN, selecione o iniciador iSCSI ou FC no host:

Neste campo…	Faça isso…
Hospedar	Clique duas vezes no nome do grupo de clusters para exibir uma lista suspensa que mostra os hosts que pertencem ao cluster e, em seguida, selecione o host para o iniciador. Este campo será exibido somente se o LUN for compartilhado por hosts em um cluster de failover do Windows Server.
Escolha o iniciador do host	Selecione **Fibre Channel** ou **iSCSI** e, em seguida, selecione o iniciador no host. Você pode selecionar vários iniciadores FC se estiver usando FC com E/S multicaminho (MPIO).

9. Na página Tipo de grupo, especifique se deseja mapear um igroup existente para o LUN ou criar um novo igroup:

Selecione…	Se…
Criar novo igroup para iniciadores selecionados	Você deseja criar um novo igroup para os iniciadores selecionados.

Selecione…	Se…
Escolha um igroup existente ou especifique um novo igroup para iniciadores selecionados	Você deseja especificar um igroup existente para os iniciadores selecionados ou criar um novo igroup com o nome especificado. Digite o nome do igroup no campo **nome do igroup**. Digite as primeiras letras do nome do igroup existente para preencher automaticamente o campo.

10. Na página Resumo, revise suas seleções e clique em **Concluir**.

    O SnapCenter cria o LUN e o conecta à unidade ou caminho de unidade especificado no host.

Redimensionar um disco

Você pode aumentar ou diminuir o tamanho de um disco conforme as necessidades do seu sistema de armazenamento mudam.

Sobre esta tarefa

- Para LUN com provisionamento fino, o tamanho da geometria do LUN ONTAP é mostrado como o tamanho máximo.
- Para LUN com provisionamento espesso, o tamanho expansível (tamanho disponível no volume) é mostrado como o tamanho máximo.
- LUNs com partições no estilo MBR têm um limite de tamanho de 2 TB.
- LUNs com partições no estilo GPT têm um limite de tamanho de sistema de armazenamento de 16 TB.
- É uma boa ideia fazer um Snapshot antes de redimensionar um LUN.
- Se você precisar restaurar um LUN de um Snapshot feito antes do LUN ser redimensionado, o SnapCenter redimensionará automaticamente o LUN para o tamanho do Snapshot.

  Após a operação de restauração, os dados adicionados ao LUN após o redimensionamento devem ser restaurados a partir de um Snapshot feito após o redimensionamento.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o host na lista suspensa Host.

   Os discos estão listados.

4. Selecione o disco que deseja redimensionar e clique em **Redimensionar**.
5. Na caixa de diálogo Redimensionar disco, use a ferramenta deslizante para especificar o novo tamanho do disco ou insira o novo tamanho no campo Tamanho.

Se você inserir o tamanho manualmente, precisará clicar fora do campo Tamanho antes que o botão Reduzir ou Expandir seja habilitado adequadamente. Além disso, você deve clicar em MB, GB ou TB para especificar a unidade de medida.

6. Quando estiver satisfeito com suas entradas, clique em **Reduzir** ou **Expandir**, conforme apropriado.

   O SnapCenter redimensiona o disco.

Conecte um disco

Você pode usar o assistente Conectar Disco para conectar um LUN existente a um host ou para reconectar um LUN que foi desconectado.

Antes de começar

- Você deve ter iniciado o serviço FC ou iSCSI no sistema de armazenamento.
- Se estiver usando iSCSI, você deverá ter estabelecido uma sessão iSCSI com o sistema de armazenamento.
- Não é possível conectar um LUN a mais de um host, a menos que o LUN seja compartilhado por hosts em um cluster de failover do Windows Server.
- Se o LUN for compartilhado por hosts em um cluster de failover do Windows Server que usa CSV (Cluster Shared Volumes), você deverá conectar o disco no host que possui o grupo de clusters.
- O Plug-in para Windows precisa ser instalado somente no host no qual você está conectando o disco.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o host na lista suspensa **Host**.
4. Clique em **Conectar**.

   O assistente Conectar disco é aberto.

5. Na página Nome do LUN, identifique o LUN ao qual deseja se conectar:

Neste campo…	Faça isso…
Sistema de armazenamento	Selecione o SVM para o LUN.
Caminho LUN	Clique em **Procurar** para selecionar o caminho completo do volume que contém o LUN.
Nome da LUN	Digite o nome do LUN.
Tamanho do cluster	Selecione o tamanho de alocação do bloco LUN para o cluster. O tamanho do cluster depende do sistema operacional e dos aplicativos.

Neste campo…	Faça isso…
Rótulo LUN	Opcionalmente, insira um texto descritivo para o LUN.

6. Na página Tipo de disco, selecione o tipo de disco:

Selecione…	Se…
Disco dedicado	O LUN pode ser acessado por apenas um host.
Disco compartilhado	O LUN é compartilhado por hosts em um cluster de failover do Windows Server. Você só precisa conectar o disco a um host no cluster de failover.
Volume compartilhado do cluster (CSV)	O LUN é compartilhado por hosts em um cluster de failover do Windows Server que usa CSV. Certifique-se de que o host no qual você está se conectando ao disco seja o proprietário do grupo de cluster.

7. Na página Propriedades da unidade, especifique as propriedades da unidade:

Propriedade	Descrição
Atribuição automática	Deixe o SnapCenter atribuir automaticamente um ponto de montagem de volume com base na unidade do sistema. Por exemplo, se a unidade do sistema for C:, a propriedade de atribuição automática criará um ponto de montagem de volume na unidade C: (C:\scmnpt\). A propriedade de atribuição automática não é suportada para discos compartilhados.
Atribuir letra de unidade	Monte o disco na unidade selecionada na lista suspensa ao lado.
Usar ponto de montagem de volume	Monte o disco no caminho da unidade especificado no campo ao lado. A raiz do ponto de montagem do volume deve pertencer ao host no qual você está criando o disco.

Propriedade	Descrição
Não atribua letra de unidade ou ponto de montagem de volume	Escolha esta opção se preferir montar o disco manualmente no Windows.

8. Na página Map LUN, selecione o iniciador iSCSI ou FC no host:

Neste campo…	Faça isso…
Hospedar	Clique duas vezes no nome do grupo de clusters para exibir uma lista suspensa que mostra os hosts que pertencem ao cluster e, em seguida, selecione o host para o iniciador. Este campo será exibido somente se o LUN for compartilhado por hosts em um cluster de failover do Windows Server.
Escolha o iniciador do host	Selecione **Fibre Channel** ou **iSCSI** e, em seguida, selecione o iniciador no host. Você pode selecionar vários iniciadores FC se estiver usando FC com MPIO.

9. Na página Tipo de grupo, especifique se deseja mapear um igroup existente para o LUN ou criar um novo igroup:

Selecione…	Se…
Criar novo igroup para iniciadores selecionados	Você deseja criar um novo igroup para os iniciadores selecionados.
Escolha um igroup existente ou especifique um novo igroup para iniciadores selecionados	Você deseja especificar um igroup existente para os iniciadores selecionados ou criar um novo igroup com o nome especificado. Digite o nome do igroup no campo **nome do igroup**. Digite as primeiras letras do nome do igroup existente para preencher o campo automaticamente.

10. Na página Resumo, revise suas seleções e clique em **Concluir**.

    O SnapCenter conecta o LUN à unidade ou caminho de unidade especificado no host.

Desconectar um disco

Você pode desconectar um LUN de um host sem afetar o conteúdo do LUN, com uma exceção: se você desconectar um clone antes que ele seja dividido, perderá o conteúdo do clone.

Antes de começar

- Certifique-se de que o LUN não esteja sendo usado por nenhum aplicativo.
- Certifique-se de que o LUN não esteja sendo monitorado com software de monitoramento.
- Se o LUN for compartilhado, certifique-se de remover as dependências de recursos do cluster do LUN e verifique se todos os nós no cluster estão ligados, funcionando corretamente e disponíveis para o SnapCenter.

Sobre esta tarefa

Se você desconectar um LUN em um volume FlexClone criado SnapCenter e nenhum outro LUN no volume estiver conectado, o SnapCenter excluirá o volume. Antes de desconectar o LUN, o SnapCenter exibe uma mensagem avisando que o volume FlexClone pode ser excluído.

Para evitar a exclusão automática do volume FlexClone , você deve renomear o volume antes de desconectar o último LUN. Ao renomear o volume, certifique-se de alterar vários caracteres além do último caractere do nome.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o host na lista suspensa **Host**.

   Os discos estão listados.
4. Selecione o disco que você deseja desconectar e clique em **Desconectar**.
5. Na caixa de diálogo Desconectar disco, clique em **OK**.

   O SnapCenter desconecta o disco.

Excluir um disco

Você pode excluir um disco quando não precisar mais dele. Depois de excluir um disco, não é possível recuperá-lo.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Discos**.
3. Selecione o host na lista suspensa **Host**.

   Os discos estão listados.
4. Selecione o disco que deseja excluir e clique em **Excluir**.
5. Na caixa de diálogo Excluir disco, clique em **OK**.

   O SnapCenter exclui o disco.

Crie e gerencie compartilhamentos SMB

Para configurar um compartilhamento SMB3 em uma máquina virtual de armazenamento

(SVM), você pode usar a interface de usuário do SnapCenter ou cmdlets do PowerShell.

Melhores práticas: o uso de cmdlets é recomendado porque permite que você aproveite os modelos fornecidos com o SnapCenter para automatizar a configuração de compartilhamento.

Os modelos encapsulam as melhores práticas para configuração de volume e compartilhamento. Você pode encontrar os modelos na pasta Modelos na pasta de instalação do Pacote de plug-ins do SnapCenter para Windows.

Se você se sentir confortável, poderá criar seus próprios modelos seguindo os modelos fornecidos. Você deve revisar os parâmetros na documentação do cmdlet antes de criar um modelo personalizado.

Criar um compartilhamento SMB

Você pode usar a página Compartilhamentos do SnapCenter para criar um compartilhamento SMB3 em uma máquina virtual de armazenamento (SVM).

Você não pode usar o SnapCenter para fazer backup de bancos de dados em compartilhamentos SMB. O suporte para PMEs é limitado apenas ao provisionamento.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Compartilhamentos**.
3. Selecione a SVM na lista suspensa **Máquina Virtual de Armazenamento**.
4. Clique em **Novo**.

   A caixa de diálogo Novo compartilhamento é aberta.

5. Na caixa de diálogo Novo compartilhamento, defina o compartilhamento:

Neste campo…	Faça isso…
Descrição	Insira um texto descritivo para o compartilhamento.
Nome do compartilhamento	Digite o nome do compartilhamento, por exemplo, test_share. O nome que você inserir para o compartilhamento também será usado como nome do volume. O nome da ação: • Deve ser uma string UTF-8. • Não deve incluir os seguintes caracteres: caracteres de controle de 0x00 a 0x1F (ambos inclusivos), 0x22 (aspas duplas) e caracteres especiais `\ / [ ] : (vertical bar) < > + = ; , ?`

Neste campo…	Faça isso…
Compartilhar caminho	• Clique no campo para inserir um novo caminho para o sistema de arquivos, por exemplo, /. • Clique duas vezes no campo para selecionar em uma lista de caminhos de sistema de arquivos existentes.

6. Quando estiver satisfeito com suas entradas, clique em **OK**.

   O SnapCenter cria o compartilhamento SMB no SVM.

Excluir um compartilhamento SMB

Você pode excluir um compartilhamento SMB quando não precisar mais dele.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Compartilhamentos**.
3. Na página Compartilhamentos, clique no campo **Máquina Virtual de Armazenamento** para exibir uma lista suspensa com uma lista de máquinas virtuais de armazenamento (SVMs) disponíveis e selecione a SVM para o compartilhamento que você deseja excluir.
4. Na lista de compartilhamentos no SVM, selecione o compartilhamento que deseja excluir e clique em **Excluir**.
5. Na caixa de diálogo Excluir compartilhamento, clique em **OK**.

   O SnapCenter exclui o compartilhamento SMB do SVM.

Recupere espaço no sistema de armazenamento

Embora o NTFS rastreie o espaço disponível em um LUN quando os arquivos são excluídos ou modificados, ele não relata as novas informações ao sistema de armazenamento. Você pode executar o cmdlet de recuperação de espaço do PowerShell no host do Plug-in para Windows para garantir que os blocos recém-liberados sejam marcados como disponíveis no armazenamento.

Se estiver executando o cmdlet em um host de plug-in remoto, você deverá executar o cmdlet SnapCenterOpen-SMConnection para abrir uma conexão com o SnapCenter Server.

Antes de começar

- Você deve garantir que o processo de recuperação de espaço tenha sido concluído antes de executar uma operação de restauração.
- Se o LUN for compartilhado por hosts em um cluster de failover do Windows Server, você deverá executar a recuperação de espaço no host que possui o grupo de clusters.
- Para um desempenho ideal de armazenamento, você deve executar a recuperação de espaço com a maior frequência possível.

Você deve garantir que todo o sistema de arquivos NTFS tenha sido verificado.

Sobre esta tarefa

- A recuperação de espaço consome muito tempo e exige muita CPU, por isso, geralmente, é melhor executar a operação quando o uso do sistema de armazenamento e do host Windows estiver baixo.
- A recuperação de espaço recupera quase todo o espaço disponível, mas não 100%.
- Você não deve executar a desfragmentação do disco ao mesmo tempo em que estiver recuperando espaço.

  Fazer isso pode atrasar o processo de recuperação.

Etapa

No prompt de comando do PowerShell do servidor de aplicativos, digite o seguinte comando:

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

drive_path é o caminho da unidade mapeado para o LUN.

Provisionar armazenamento usando cmdlets do PowerShell

Se não quiser usar a GUI do SnapCenter para executar tarefas de provisionamento de host e recuperação de espaço, você pode usar os cmdlets do PowerShell. Você pode usar cmdlets diretamente ou adicioná-los a scripts.

Se estiver executando os cmdlets em um host de plug-in remoto, você deverá executar o cmdlet SnapCenter Open-SMConnection para abrir uma conexão com o SnapCenter Server.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Se os cmdlets do SnapCenter PowerShell estiverem quebrados devido à remoção do SnapDrive para Windows do servidor, consulte "Os cmdlets do SnapCenter são interrompidos quando o SnapDrive para Windows é desinstalado" .

Provisionar armazenamento em ambientes VMware

Você pode usar o SnapCenter Plug-in para Microsoft Windows em ambientes VMware para criar e gerenciar LUNs e gerenciar Snapshots.

Plataformas de sistema operacional convidado VMware suportadas

- Versões suportadas do Windows Server
- Configurações de cluster da Microsoft

  Suporte para até 16 nós suportados no VMware ao usar o Microsoft iSCSI Software Initiator ou até dois nós usando FC

- LUNs RDM

Suporte para um máximo de 56 LUNs RDM com quatro controladores LSI Logic SCSI para RDMS normal ou 42 LUNs RDM com três controladores LSI Logic SCSI em um plug-in VMware VM MSCS box-to-box para configuração do Windows

Suporta o controlador SCSI VMware ParaVirtual. 256 discos podem ser suportados em discos RDM.

Para obter as informações mais recentes sobre as versões suportadas, consulte "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Limitações relacionadas ao servidor VMware ESXi

- A instalação do Plug-in para Windows em um cluster da Microsoft em máquinas virtuais usando credenciais ESXi não é suportada.

  Você deve usar suas credenciais do vCenter ao instalar o Plug-in para Windows em máquinas virtuais em cluster.

- Todos os nós em cluster devem usar o mesmo ID de destino (no adaptador SCSI virtual) para o mesmo disco em cluster.
- Ao criar um RDM LUN fora do Plug-in para Windows, você deve reiniciar o serviço do plug-in para que ele reconheça o disco recém-criado.
- Não é possível usar iniciadores iSCSI e FC ao mesmo tempo em um sistema operacional convidado VMware.

Privilégios mínimos do vCenter necessários para operações do SnapCenter RDM

Você deve ter os seguintes privilégios do vCenter no host para executar operações RDM em um sistema operacional convidado:

- Armazenamento de dados: Remover arquivo
- Host: Configuração > Configuração da partição de armazenamento
- Máquina Virtual: Configuração

Você deve atribuir esses privilégios a uma função no nível do Virtual Center Server. A função à qual você atribui esses privilégios não pode ser atribuída a nenhum usuário sem privilégios de root.

Depois de atribuir esses privilégios, você pode instalar o Plug-in para Windows no sistema operacional convidado.

Gerenciar LUNs FC RDM em um cluster Microsoft

Você pode usar o Plug-in para Windows para gerenciar um cluster Microsoft usando LUNs FC RDM, mas primeiro você deve criar o quorum RDM compartilhado e o armazenamento compartilhado fora do plug-in e, em seguida, adicionar os discos às máquinas virtuais no cluster.

A partir do ESXi 5.5, você também pode usar hardware ESX iSCSI e FCoE para gerenciar um cluster Microsoft. O plug-in para Windows inclui suporte pronto para uso para clusters da Microsoft.

Requisitos

O plug-in para Windows fornece suporte para clusters da Microsoft usando LUNs FC RDM em duas máquinas virtuais diferentes que pertencem a dois servidores ESX ou ESXi diferentes, também conhecidos como cluster entre caixas, quando você atende a requisitos de configuração específicos.

- As máquinas virtuais (VMs) devem estar executando a mesma versão do Windows Server.
- As versões do servidor ESX ou ESXi devem ser as mesmas para cada host pai VMware.
- Cada host pai deve ter pelo menos dois adaptadores de rede.
- Deve haver pelo menos um armazenamento de dados do VMware Virtual Machine File System (VMFS) compartilhado entre os dois servidores ESX ou ESXi.
- A VMware recomenda que o armazenamento de dados compartilhado seja criado em um FC SAN.

  Se necessário, o armazenamento de dados compartilhado também pode ser criado via iSCSI.
- O LUN RDM compartilhado deve estar no modo de compatibilidade física.
- O LUN RDM compartilhado deve ser criado manualmente fora do Plug-in para Windows.

  Você não pode usar discos virtuais para armazenamento compartilhado.
- Um controlador SCSI deve ser configurado em cada máquina virtual no cluster no modo de compatibilidade física:

  O Windows Server 2008 R2 exige que você configure o controlador LSI Logic SAS SCSI em cada máquina virtual. LUNs compartilhados não podem usar o controlador SAS LSI Logic existente se houver apenas um de seu tipo e ele já estiver conectado à unidade C:.

  Controladores SCSI do tipo paravirtual não são suportados em clusters VMware Microsoft.

  > Ao adicionar um controlador SCSI a um LUN compartilhado em uma máquina virtual no modo de compatibilidade física, você deve selecionar a opção **Raw Device Mappings** (RDM) e não a opção **Criar um novo disco** no VMware Infrastructure Client.
- Os clusters de máquinas virtuais da Microsoft não podem fazer parte de um cluster VMware.
- Você deve usar credenciais do vCenter e não credenciais do ESX ou ESXi ao instalar o Plug-in para Windows em máquinas virtuais que pertencem a um cluster da Microsoft.
- O Plug-in para Windows não pode criar um único igroup com iniciadores de vários hosts.

  O igroup contendo os iniciadores de todos os hosts ESXi deve ser criado no controlador de armazenamento antes de criar os LUNs RDM que serão usados como discos de cluster compartilhados.
- Certifique-se de criar um RDM LUN no ESXi 5.0 usando um iniciador FC.

  Quando você cria um RDM LUN, um grupo iniciador é criado com ALUA.

Limitações

O plug-in para Windows oferece suporte a clusters da Microsoft usando LUNs RDM FC/iSCSI em diferentes máquinas virtuais pertencentes a diferentes servidores ESX ou ESXi.

> Este recurso não é suportado em versões anteriores ao ESX 5.5i.

- O plug-in para Windows não oferece suporte a clusters em datastores ESX iSCSI e NFS.
- O Plug-in para Windows não oferece suporte a iniciadores mistos em um ambiente de cluster.

  Os iniciadores devem ser FC ou Microsoft iSCSI, mas não ambos.

- Os iniciadores iSCSI e HBAs do ESX não são suportados em discos compartilhados em um cluster da Microsoft.
- O plug-in para Windows não oferece suporte à migração de máquina virtual com o vMotion se a máquina virtual fizer parte de um cluster da Microsoft.
- O plug-in para Windows não oferece suporte a MPIO em máquinas virtuais em um cluster da Microsoft.

Criar um FC RDM LUN compartilhado

Antes de poder usar LUNs FC RDM para compartilhar armazenamento entre nós em um cluster Microsoft, você deve primeiro criar o disco de quorum compartilhado e o disco de armazenamento compartilhado e, em seguida, adicioná-los às duas máquinas virtuais no cluster.

O disco compartilhado não é criado usando o Plug-in para Windows. Você deve criar e adicionar o LUN compartilhado a cada máquina virtual no cluster. Para obter informações, consulte "Agrupar máquinas virtuais em hosts físicos" .

Adicionar licenças baseadas no controlador SnapCenter Standard

Uma licença baseada em controlador SnapCenter Standard será necessária se você estiver usando controladores de armazenamento FAS, AFF ou ASA .

A licença baseada em controlador tem as seguintes características:

- O direito ao SnapCenter Standard está incluído na compra do Premium ou Flash Bundle (não no pacote básico)
- Uso de armazenamento ilimitado
- Adicionado diretamente ao controlador de armazenamento FAS, AFF ou ASA usando o ONTAP System Manager ou o ONTAP CLI.

> Não insira nenhuma informação de licença na interface do usuário do SnapCenter para as licenças baseadas no controlador SnapCenter .

- Bloqueado no número de série do controlador

Para obter informações sobre as licenças necessárias, consulte"Licenças SnapCenter" .

Etapa 1: Verifique se a licença do SnapManager Suite está instalada

Você pode usar a interface de usuário do SnapCenter para verificar se uma licença do SnapManager Suite está instalada nos sistemas de armazenamento primário FAS, AFF ou ASA e identificar quais sistemas precisam de licenças. As licenças do SnapManager Suite se aplicam somente a SVMs FAS, AFF e ASA ou clusters em sistemas de armazenamento primário.

> Se você já tiver uma licença do SnapManager Suite no seu controlador, o SnapCenter fornecerá automaticamente o direito à licença baseada no controlador padrão. Os nomes licença SnapManagerSuite e licença baseada em controlador SnapCenter Standard são usados de forma intercambiável, mas se referem à mesma licença.

Passos

1. No painel de navegação esquerdo, selecione **Sistemas de armazenamento**.

2. Na página Sistemas de Armazenamento, no menu suspenso **Tipo**, selecione se deseja visualizar todos os SVMs ou clusters que foram adicionados:
   - Para visualizar todos os SVMs que foram adicionados, selecione * ONTAP SVMs*.
   - Para visualizar todos os clusters que foram adicionados, selecione * Clusters ONTAP *.

     Quando você seleciona o nome do cluster, todas as SVMs que fazem parte do cluster são exibidas na seção Máquinas Virtuais de Armazenamento.
3. Na lista Conexões de armazenamento, localize a coluna Licença do controlador.

   A coluna Licença do Controlador exibe o seguinte status:

   -  indica que uma licença do SnapManager Suite está instalada em um sistema de armazenamento primário FAS, AFF ou ASA .
   -  indica que uma licença do SnapManager Suite não está instalada em um sistema de armazenamento primário FAS, AFF ou ASA .
   - Não aplicável indica que uma licença do SnapManager Suite não é aplicável porque o controlador de armazenamento está no Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select ou secundário.

Etapa 2: Identificar as licenças instaladas no controlador

Você pode usar a linha de comando ONTAP para visualizar todas as licenças instaladas no seu controlador. Você deve ser um administrador de cluster no sistema FAS, AFF ou ASA .

O controlador exibe a licença baseada no controlador SnapCenter Standard como a licença SnapManagerSuite.

Passos

1. Efetue login no controlador NetApp usando a linha de comando ONTAP .
2. Digite o comando license show e visualize a saída para ver se a licença do SnapManagerSuite está instalada.

Exemplo de saída

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

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

Serial Number: 1-81-0000000000000000000000000xx
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 -
```

No exemplo, a licença SnapManagerSuite está instalada, portanto, nenhuma ação adicional de licenciamento do SnapCenter é necessária.

Etapa 3: recuperar o número de série do controlador

Obtenha o número de série do controlador usando a linha de comando ONTAP . Você deve ser um administrador de cluster no sistema FAS, AFF ou ASA para obter seu número de série de licença baseado em controlador.

Passos

1. Efetue login no controlador usando a linha de comando ONTAP .
2. Digite o comando show -instance do sistema e revise a saída para localizar o número de série do controlador.

Exemplo de saída

```
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: xxxxxxxxx
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: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. Registre os números de série.

Etapa 4: recuperar o número de série da licença baseada no controlador

Se estiver usando armazenamento FAS, ASA ou AFF , você poderá recuperar a licença baseada no controlador SnapCenter no site de suporte da NetApp antes de instalá-lo usando a linha de comando ONTAP .

Antes de começar

- Você deve ter credenciais de login válidas no site de suporte da NetApp .

  Se você não inserir credenciais válidas, o sistema não retornará nenhuma informação para sua pesquisa.

- Você deve ter o número de série do controlador.

Passos

1. Faça login no "Site de suporte da NetApp" .
2. Navegue até **Sistemas** > **Licenças de software**.
3. Na área Critérios de seleção, certifique-se de que o Número de série (localizado na parte traseira da unidade) esteja selecionado, insira o número de série do controlador e selecione **Ir!**.

Uma lista de licenças para o controlador especificado é exibida.

4. Localize e registre a licença do SnapCenter Standard ou SnapManagerSuite.

Etapa 5: adicionar licença baseada em controlador

Você pode usar a linha de comando ONTAP para adicionar uma licença baseada no controlador SnapCenter quando estiver usando sistemas FAS, AFF ou ASA e tiver uma licença SnapCenter Standard ou SnapManagerSuite.

Antes de começar

- Você deve ser um administrador de cluster no sistema FAS, AFF ou ASA .
- Você deve ter a licença SnapCenter Standard ou SnapManagerSuite.

Sobre esta tarefa

Se você quiser instalar o SnapCenter em caráter de teste com armazenamento FAS, AFF ou ASA , poderá obter uma licença de avaliação do Premium Bundle para instalar no seu controlador.

Se você quiser instalar o SnapCenter em caráter de teste, entre em contato com seu representante de vendas para obter uma licença de avaliação do Premium Bundle para instalar no seu controlador.

Passos

1. Efetue login no cluster NetApp usando a linha de comando ONTAP .
2. Adicione a chave de licença do SnapManagerSuite:

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

   Este comando está disponível no nível de privilégio de administrador.

3. Verifique se a licença do SnapManagerSuite está instalada:

   ```
   license show
   ```

Etapa 6: Remova a licença de teste

Se você estiver usando uma licença SnapCenter Standard baseada em controlador e precisar remover a licença de teste baseada em capacidade (número de série terminando em “50”), use os comandos MySQL para remover a licença de teste manualmente. A licença de teste não pode ser excluída usando a interface de usuário do SnapCenter .

> A remoção manual de uma licença de avaliação só é necessária se você estiver usando uma licença baseada no controlador SnapCenter Standard.

Passos

1. No SnapCenter Server, abra uma janela do PowerShell para redefinir a senha do MySQL.
   a. Execute o cmdlet Open-SmConnection para estabelecer conexão com o SnapCenter Server para uma conta SnapCenterAdmin.
   b. Execute o Set-SmRepositoryPassword para redefinir a senha do MySQL.

      Para obter informações sobre os cmdlets, consulte "Guia de referência do cmdlet do software SnapCenter" .
2. Abra o prompt de comando e execute mysql -u root -p para efetuar login no MySQL.

   O MySQL solicita a senha. Insira as credenciais que você forneceu ao redefinir a senha.
3. Remova a licença de teste do banco de dados:

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

Configurar alta disponibilidade

Configurar servidores SnapCenter para alta disponibilidade

Para oferecer suporte à Alta Disponibilidade (HA) no SnapCenter em execução no Windows ou no Linux, você pode instalar o balanceador de carga F5. O F5 permite que o SnapCenter Server suporte configurações ativas-passivas em até dois hosts que estão no mesmo local. Para usar o F5 Load Balancer no SnapCenter, você deve configurar os servidores SnapCenter e configurar o balanceador de carga F5.

Você também pode configurar o Balanceamento de Carga de Rede (NLB) para configurar a Alta Disponibilidade do SnapCenter . Você deve configurar manualmente o NLB fora da instalação do SnapCenter para alta disponibilidade.

Para o ambiente de nuvem, você pode configurar alta disponibilidade usando o Amazon Web Services (AWS) Elastic Load Balancing (ELB) e o balanceador de carga do Azure.

Configurar alta disponibilidade usando F5

Para obter instruções sobre como configurar os servidores SnapCenter para alta disponibilidade usando o balanceador de carga F5, consulte "Como configurar servidores SnapCenter para alta disponibilidade usando o balanceador de carga F5" .

Você deve ser membro do grupo Administradores locais nos servidores SnapCenter (além de ter a função SnapCenterAdmin atribuída) para usar os seguintes cmdlets para adicionar e remover clusters F5:

- Adicionar-SmServerCluster
- Adicionar-SmServer
- Remover-SmServerCluster

  Para obter mais informações, consulte "Guia de referência do cmdlet do software SnapCenter" .

Informações adicionais

- Depois de instalar e configurar o SnapCenter para alta disponibilidade, edite o atalho da área de trabalho do SnapCenter para apontar para o IP do cluster F5.
- Se ocorrer um failover entre os servidores SnapCenter e se também houver uma sessão SnapCenter existente, você deverá fechar o navegador e fazer logon no SnapCenter novamente.
- Na configuração do balanceador de carga (NLB ou F5), se você adicionar um host que é parcialmente resolvido pelo host NLB ou F5 e se o host SnapCenter não conseguir contatá-lo, a página do host SnapCenter alternará frequentemente entre os hosts inativos e em execução. Para resolver esse problema, você deve garantir que ambos os hosts do SnapCenter consigam resolver o host no NLB ou no host F5.
- Os comandos do SnapCenter para configurações de MFA devem ser executados em todos os hosts. A configuração da parte confiável deve ser feita no servidor dos Serviços de Federação do Active Directory (AD FS) usando detalhes do cluster F5. O acesso à interface de usuário do SnapCenter no nível do host será bloqueado após a ativação do MFA.
- Durante o failover, as configurações do log de auditoria não serão refletidas no segundo host. Portanto, você deve repetir manualmente as configurações do log de auditoria no host passivo F5 quando ele se tornar ativo.

Configurar alta disponibilidade usando balanceamento de carga de rede (NLB)

Você pode configurar o Balanceamento de Carga de Rede (NLB) para configurar a Alta Disponibilidade do SnapCenter . Você deve configurar manualmente o NLB fora da instalação do SnapCenter para alta disponibilidade.

Para obter informações sobre como configurar o balanceamento de carga de rede (NLB) com o SnapCenter , consulte "Como configurar o NLB com o SnapCenter" .

Configurar alta disponibilidade usando o AWS Elastic Load Balancing (ELB)

Você pode configurar o ambiente SnapCenter de alta disponibilidade na Amazon Web Services (AWS) configurando dois servidores SnapCenter em zonas de disponibilidade (AZs) separadas e configurando-os para failover automático. A arquitetura inclui endereços IP privados virtuais, tabelas de roteamento e sincronização entre bancos de dados MySQL ativos e em espera.

Passos

1. Configurar sobreposição de IP virtual privado na AWS. Para obter informações, consulte "Configurar sobreposição de IP virtual privado" .
2. Prepare seu host Windows
   a. Forçar o IPv4 a ser priorizado em relação ao IPv6:
      - Localização: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
      - Chave: DisabledComponents
      - Tipo: REG_DWORD
      - Valor: 0x20
   b. Certifique-se de que os nomes de domínio totalmente qualificados possam ser resolvidos via DNS ou via configuração de host local para endereços IPv4.
   c. Certifique-se de que você não tenha um proxy de sistema configurado.
   d. Certifique-se de que a senha do administrador seja a mesma no Windows Server ao usar uma configuração sem um Active Directory e que os servidores não estejam no mesmo domínio.
   e. Adicione IP virtual em ambos os servidores Windows.
3. Crie o cluster SnapCenter .
   a. Inicie o Powershell e conecte-se ao SnapCenter.
      ```
      Open-SmConnection
      ```
   b. Crie o cluster.
      ```
      Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip>
      -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator
      ```
   c. Adicione o servidor secundário.
      ```
      Add-SmServer -ServerName <server_name> -ServerIP <server_ip>
      -CleanUpSecondaryServer -Verbose -Credential administrator
      ```
   d. Obtenha os detalhes de alta disponibilidade.
      ```
      Get-SmServerConfig
      ```
4. Crie a função Lamda para ajustar a tabela de roteamento caso o ponto de extremidade do IP privado virtual fique indisponível, monitorado pelo AWS CloudWatch. Para obter informações, consulte "Criar uma função Lambda" .
5. Crie um monitor no CloudWatch para monitorar a disponibilidade do endpoint do SnapCenter . Um alarme é configurado para acionar uma função Lambda se o ponto de extremidade estiver inacessível. A função Lambda ajusta a tabela de roteamento para redirecionar o tráfego para o servidor SnapCenter ativo. Para obter informações, consulte "Crie canários sintéticos" .
6. Implemente o fluxo de trabalho usando uma função de etapa como alternativa ao monitoramento do CloudWatch, proporcionando tempos de failover menores. O fluxo de trabalho inclui uma função de sonda Lambda para testar o URL do SnapCenter , uma tabela do DynamoDB para armazenar contagens de falhas e a própria função Step.
   a. Use uma função lambda para sondar o URL do SnapCenter . Para obter informações, consulte "Criar função Lambda" .
   b. Crie uma tabela do DynamoDB para armazenar a contagem de falhas entre duas iterações da Função de Etapa. Para obter informações, consulte "Comece a usar a tabela do DynamoDB" .
   c. Crie a função Step. Para obter informações, consulte "Documentação da função Step" .
   d. Teste uma única etapa.

e. Teste a função completa.

f. Crie uma função do IAM e ajuste as permissões para poder executar a função do Lambda.

g. Crie uma programação para acionar a Step Function. Para obter informações, consulte "Usando o Amazon EventBridge Scheduler para iniciar um Step Functions" .

Configurar alta disponibilidade usando o balanceador de carga do Azure

Você pode configurar o ambiente SnapCenter de alta disponibilidade usando o balanceador de carga do Azure.

Passos

1. Crie máquinas virtuais em um conjunto de dimensionamento usando o portal do Azure. O conjunto de dimensionamento de máquinas virtuais do Azure permite que você crie e gerencie um grupo de máquinas virtuais com balanceamento de carga. O número de instâncias de máquinas virtuais pode aumentar ou diminuir automaticamente em resposta à demanda ou a um cronograma definido. Para obter informações, consulte "Crie máquinas virtuais em um conjunto de dimensionamento usando o portal do Azure" .
2. Depois de configurar as máquinas virtuais, efetue login em cada máquina virtual no conjunto de VMs e instale o SnapCenter Server em ambos os nós.
3. Crie o cluster no host 1.
   ```
   Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>
   ```
4. Adicione o servidor secundário.
   ```
   Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>
   ```
5. Obtenha os detalhes de alta disponibilidade.
   ```
   Get-SmServerConfig
   ```
6. Se necessário, reconstrua o host secundário.
   ```
   Set-SmRepositoryConfig -RebuildSlave -Verbose
   ```
7. Failover para o segundo host.
   ```
   Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose
   ```

== Mude de NLB para F5 para alta disponibilidade

Você pode alterar a configuração do SnapCenter HA do Network Load Balancing (NLB) para usar o F5 Load Balancer.

Passos

1. Configure os servidores SnapCenter para alta disponibilidade usando F5. "Saber mais" .
2. No host do SnapCenter Server, inicie o PowerShell.
3. Inicie uma sessão usando o cmdlet Open-SmConnection e insira suas credenciais.
4. Atualize o SnapCenter Server para apontar para o endereço IP do cluster F5 usando o cmdlet Update-SmServerCluster.

   As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Alta disponibilidade para o repositório SnapCenter MySQL

A replicação do MySQL é um recurso do MySQL Server que permite replicar dados de um servidor de banco de dados MySQL (mestre) para outro servidor de banco de dados MySQL (escravo). O SnapCenter oferece suporte à replicação do MySQL para alta disponibilidade somente em dois nós habilitados para balanceamento de carga de rede (NLB).

O SnapCenter executa operações de leitura ou gravação no repositório mestre e roteia sua conexão para o repositório escravo quando há uma falha no repositório mestre. O repositório escravo então se torna o repositório mestre. O SnapCenter também oferece suporte à replicação reversa, que é ativada somente durante o failover.

Se você quiser usar o recurso de alta disponibilidade (HA) do MySQL, deverá configurar o Network Load Balancer (NLB) no primeiro nó. O repositório MySQL é instalado neste nó como parte da instalação. Ao instalar o SnapCenter no segundo nó, você deve ingressar no F5 do primeiro nó e criar uma cópia do repositório MySQL no segundo nó.

O SnapCenter fornece os cmdlets *Get-SmRepositoryConfig* e *Set-SmRepositoryConfig* do PowerShell para gerenciar a replicação do MySQL.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Você deve estar ciente das limitações relacionadas ao recurso MySQL HA:

- NLB e MySQL HA não são suportados além de dois nós.
- Não há suporte para alternar de uma instalação autônoma do SnapCenter para uma instalação NLB ou vice-versa e alternar de uma configuração autônoma do MySQL para o MySQL HA.
- O failover automático não será suportado se os dados do repositório escravo não estiverem sincronizados com os dados do repositório mestre.

  Você pode iniciar um failover forçado usando o cmdlet *Set-SmRepositoryConfig*.

- Quando o failover é iniciado, os trabalhos em execução podem falhar.

  Se o failover ocorrer porque o MySQL Server ou o SnapCenter Server estiver inativo, todos os trabalhos em execução poderão falhar. Após a falha no segundo nó, todos os trabalhos subsequentes são executados com sucesso.

Para obter informações sobre como configurar alta disponibilidade, consulte "Como configurar NLB e ARR com SnapCenter" .

Configurar o controle de acesso baseado em função (RBAC)

Criar uma função

Além de usar as funções existentes do SnapCenter , você pode criar suas próprias funções e personalizar as permissões.

Para criar suas próprias funções, é necessário efetuar login como a função "SnapCenterAdmin".

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Funções**.
3. Clique + .
4. Especifique um nome e uma descrição para a nova função.

   Somente os seguintes caracteres especiais podem ser usados em nomes de usuários e grupos: espaço ( ), hífen (-), sublinhado (_) e dois pontos (:).

5. Selecione **Todos os membros desta função podem ver os objetos de outros membros** para permitir que outros membros da função vejam recursos como volumes e hosts depois de atualizarem a lista de recursos.

   Você deve desmarcar esta opção se não quiser que os membros desta função vejam objetos aos quais outros membros estão atribuídos.

   Quando esta opção está habilitada, não é necessário atribuir aos usuários acesso a objetos ou recursos se eles pertencerem à mesma função que o usuário que criou os objetos ou recursos.

6. Na página Permissões, selecione as permissões que deseja atribuir à função ou clique em **Selecionar tudo** para conceder todas as permissões à função.
7. Clique em **Enviar**.

Adicionar uma função NetApp ONTAP RBAC usando comandos de login de segurança

Você pode usar os comandos de login de segurança para adicionar uma função NetApp ONTAP RBAC quando seus sistemas de armazenamento estiverem executando o ONTAP em cluster.

Antes de começar

- Identifique a tarefa (ou tarefas) que você deseja executar e os privilégios necessários para executá-las.
- Conceda privilégios a comandos e/ou diretórios de comandos.

  Há dois níveis de acesso para cada comando/diretório de comando: acesso total e somente leitura.

  Você deve sempre atribuir os privilégios de acesso total primeiro.

- Atribuir funções aos usuários.
- Identifique sua configuração dependendo se seus plug-ins do SnapCenter estão conectados ao IP do administrador do cluster para todo o cluster ou diretamente conectados a uma SVM dentro do cluster.

Sobre esta tarefa

Para simplificar a configuração dessas funções em sistemas de armazenamento, você pode usar a ferramenta RBAC User Creator for NetApp ONTAP , publicada no Fórum de Comunidades da NetApp .

Esta ferramenta gerencia automaticamente a configuração correta dos privilégios do ONTAP . Por exemplo, a ferramenta RBAC User Creator for NetApp ONTAP adiciona automaticamente os privilégios na ordem correta para que os privilégios de acesso total apareçam primeiro. Se você adicionar primeiro os privilégios somente leitura e depois adicionar os privilégios de acesso total, o ONTAP marcará os privilégios de acesso total como

duplicados e os ignorará.

> Se você atualizar posteriormente o SnapCenter ou o ONTAP, execute novamente a ferramenta RBAC User Creator for NetApp ONTAP para atualizar as funções de usuário criadas anteriormente. Funções de usuário criadas para uma versão anterior do SnapCenter ou ONTAP não funcionam corretamente com versões atualizadas. Quando você executa a ferramenta novamente, ela realiza a atualização automaticamente. Você não precisa recriar as funções.

Para obter mais informações sobre como configurar funções ONTAP RBAC, consulte "Guia de autenticação de administrador do ONTAP 9 e RBAC Power" .

Passos

1. No sistema de armazenamento, crie uma nova função inserindo o seguinte comando:

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

   - svm_name é o nome do SVM. Se você deixar em branco, o padrão será o administrador do cluster.
   - role_name é o nome que você especifica para a função.
   - comando é o recurso ONTAP .

   > Você deve repetir este comando para cada permissão. Lembre-se de que os comandos de acesso total devem ser listados antes dos comandos somente leitura.

   Para obter informações sobre a lista de permissões, consulte"Comandos ONTAP CLI para criar funções e atribuir permissões" .

2. Crie um nome de usuário digitando o seguinte comando:

   ```
   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 é o nome do usuário que você está criando.
   - <senha> é sua senha. Se você não especificar uma senha, o sistema solicitará uma.
   - svm_name é o nome do SVM.

3. Atribua a função ao usuário digitando o seguinte comando:

   ```
   security login modify username <user_name\> -vserver <svm_name\> -role
   <role_name\> -application ontapi -application console -authmethod <password\>
   ```

   - <user_name> é o nome do usuário que você criou na Etapa 2. Este comando permite que você modifique o usuário para associá-lo à função.
   - <svm_name> é o nome do SVM.
   - <role_name> é o nome da função que você criou na Etapa 1.
   - <senha> é sua senha. Se você não especificar uma senha, o sistema solicitará uma.

4. Verifique se o usuário foi criado corretamente digitando o seguinte comando:

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

user_name é o nome do usuário que você criou na Etapa 3.

Crie funções SVM com privilégios mínimos

Há vários comandos ONTAP CLI que você deve executar ao criar uma função para um novo usuário SVM no ONTAP. Essa função é necessária se você configurar SVMs no ONTAP para usar com o SnapCenter e não quiser usar a função vsadmin.

Passos

1. No sistema de armazenamento, crie uma função e atribua todas as permissões a ela.

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

   Você deve repetir este comando para cada permissão.

2. Crie um usuário e atribua a função a ele.

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

3. Desbloqueie o usuário.

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

Comandos ONTAP CLI para criar funções SVM e atribuir permissões

Há vários comandos ONTAP CLI que você deve executar para criar funções SVM e atribuir permissões.

- `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`

Criar funções SVM para sistemas ASA r2

Há vários comandos ONTAP CLI que você deve executar para criar uma função para um

novo usuário SVM em sistemas ASA r2. Essa função é necessária se você configurar SVMs em sistemas ASA r2 para usar com o SnapCenter e não quiser usar a função vsadmin.

Passos

1. No sistema de armazenamento, crie uma função e atribua todas as permissões a ela.

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

   Você deve repetir este comando para cada permissão.

2. Crie um usuário e atribua a função a ele.

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

3. Desbloqueie o usuário.

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

Comandos ONTAP CLI para criar funções SVM e atribuir permissões

Há vários comandos ONTAP CLI que você deve executar para criar funções SVM e atribuir permissões.

- `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`

Crie funções de cluster ONTAP com privilégios mínimos

Você deve criar uma função de cluster ONTAP com privilégios mínimos para não precisar usar a função de administrador ONTAP para executar operações no SnapCenter. Você pode executar vários comandos ONTAP CLI para criar a função de cluster ONTAP e atribuir privilégios mínimos.

Passos

1. No sistema de armazenamento, crie uma função e atribua todas as permissões a ela.

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

   Você deve repetir este comando para cada permissão.

2. Crie um usuário e atribua a função a ele.

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

3. Desbloqueie o usuário.

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

Comandos ONTAP CLI para criar funções de cluster e atribuir permissões

Há vários comandos ONTAP CLI que você deve executar para criar funções de cluster e atribuir permissões.

- `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

Criar funções de cluster ONTAP para sistemas ASA r2

Você deve criar uma função de cluster ONTAP com privilégios mínimos para não precisar usar a função de administrador ONTAP para executar operações no SnapCenter. Você pode executar vários comandos ONTAP CLI para criar a função de cluster ONTAP e atribuir privilégios mínimos.

Passos

1. No sistema de armazenamento, crie uma função e atribua todas as permissões a ela.

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

   Você deve repetir este comando para cada permissão.

2. Crie um usuário e atribua a função a ele.

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

3. Desbloqueie o usuário.

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

Comandos ONTAP CLI para criar funções de cluster e atribuir permissões

Há vários comandos ONTAP CLI que você deve executar para criar funções de cluster e atribuir permissões.

- `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`

Adicionar um usuário ou grupo e atribuir função e ativos

Para configurar o controle de acesso baseado em função para usuários do SnapCenter , você pode adicionar usuários ou grupos e atribuir uma função. A função determina as opções que os usuários do SnapCenter podem acessar.

Antes de começar

- Você deve ter efetuado login com a função "SnapCenterAdmin".
- Você deve ter criado as contas de usuário ou grupo no Active Directory no sistema operacional ou banco de dados. Você não pode usar o SnapCenter para criar essas contas.

  Você pode incluir somente os seguintes caracteres especiais em nomes de usuários e grupos: espaço ( ), hífen (-), sublinhado (_) e dois pontos (:).

- O SnapCenter inclui várias funções predefinidas.

  Você pode atribuir essas funções ao usuário ou criar novas funções.

- Usuários e grupos do AD adicionados ao SnapCenter RBAC devem ter permissão de LEITURA no contêiner de usuários e no contêiner de computadores no Active Directory.
- Depois de atribuir uma função a um usuário ou grupo que contém as permissões apropriadas, você deve atribuir ao usuário acesso aos ativos do SnapCenter , como hosts e conexões de armazenamento.

  Isso permite que os usuários executem as ações para as quais têm permissão nos ativos atribuídos a eles.

- Você deve atribuir uma função ao usuário ou grupo em algum momento para aproveitar as permissões e eficiências do RBAC.
- Você pode atribuir ativos como host, grupos de recursos, política, conexão de armazenamento, plug-in e credencial ao usuário ao criar o usuário ou grupo.
- Os ativos mínimos que você deve atribuir a um usuário para executar determinadas operações são os seguintes:

Operação	Atribuição de ativos
Proteja os recursos	anfitrião, política
Backup	host, grupo de recursos, política

Operação	Atribuição de ativos
Restaurar	host, grupo de recursos
Clone	host, grupo de recursos, política
Ciclo de vida do clone	hospedar
Criar um Grupo de Recursos	hospedar

- Quando um novo nó é adicionado a um cluster do Windows ou a um ativo DAG (Exchange Server Database Availability Group) e se esse novo nó for atribuído a um usuário, você deve reatribuir o ativo ao usuário ou grupo para incluir o novo nó ao usuário ou grupo.

  Você deve reatribuir o usuário ou grupo RBAC ao cluster ou DAG para incluir o novo nó ao usuário ou grupo RBAC. Por exemplo, você tem um cluster de dois nós e atribuiu um usuário ou grupo RBAC ao cluster. Ao adicionar outro nó ao cluster, você deve reatribuir o usuário ou grupo RBAC ao cluster para incluir o novo nó para o usuário ou grupo RBAC.

- Se você estiver planejando replicar Snapshots, deverá atribuir a conexão de armazenamento para o volume de origem e de destino ao usuário que está executando a operação.

  Você deve adicionar ativos antes de atribuir acesso aos usuários.

Se estiver usando as funções do SnapCenter Plug-in for VMware vSphere para proteger VMs, VMDKs ou datastores, você deverá usar a GUI do VMware vSphere para adicionar um usuário do vCenter a uma função do SnapCenter Plug-in for VMware vSphere . Para obter informações sobre funções do VMware vSphere, consulte "Funções predefinidas incluídas no SnapCenter Plug-in for VMware vSphere" .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Usuários e acesso** > * *.
3. Na página Adicionar usuários/grupos do Active Directory ou grupo de trabalho:

Para este campo…	Faça isso…
Tipo de acesso	Selecione Domínio ou grupo de trabalho Para o tipo de autenticação de domínio, você deve especificar o nome de domínio do usuário ou grupo ao qual deseja adicionar o usuário a uma função. Por padrão, ele é pré-preenchido com o nome de domínio conectado. Você deve registrar o domínio não confiável na página **Configurações** > **Configurações globais** > **Configurações de domínio**.
Tipo	Selecione Usuário ou Grupo O SnapCenter suporta apenas o grupo de segurança e não o grupo de distribuição.
Nome de usuário	a. Digite o nome de usuário parcial e clique em **Adicionar**. O nome de usuário diferencia maiúsculas de minúsculas. b. Selecione o nome de usuário na lista de pesquisa. Ao adicionar usuários de um domínio diferente ou de um domínio não confiável, você deve digitar o nome do usuário completo, pois não há lista de pesquisa para usuários de vários domínios. Repita esta etapa para adicionar usuários ou grupos adicionais à função selecionada.
Funções	Selecione a função à qual você deseja adicionar o usuário.

4. Clique em **Atribuir** e, em seguida, na página Atribuir ativos:
   a. Selecione o tipo de ativo na lista suspensa **Ativo**.
   b. Na tabela Ativos, selecione o ativo.

      Os ativos são listados somente se o usuário os tiver adicionado ao SnapCenter.

c. Repita esse procedimento para todos os ativos necessários.

d. Clique em **Salvar**.

5. Clique em **Enviar**.

Depois de adicionar usuários ou grupos e atribuir funções, atualize a lista de recursos.

Configurar definições de log de auditoria

Os logs de auditoria são gerados para cada atividade do SnapCenter Server. Por padrão, os logs de auditoria são protegidos no local de instalação padrão *C:\Arquivos de Programas\ NetApp\ SnapCenter WebApp\audit*.

Os logs de auditoria são protegidos por meio da geração de um resumo assinado digitalmente para cada evento de auditoria para protegê-lo de modificações não autorizadas. Os resumos gerados são mantidos no arquivo de soma de verificação de auditoria separado e passam por verificações periódicas de integridade para garantir a integridade do conteúdo.

Você deve ter efetuado login com a função "SnapCenterAdmin".

Sobre esta tarefa

- Os alertas são enviados nos seguintes cenários:
  - A verificação da integridade do log de auditoria ou o servidor Syslog está habilitado ou desabilitado
  - Verificação de integridade do log de auditoria, log de auditoria ou falha do log do servidor Syslog
  - Pouco espaço em disco
- O e-mail é enviado somente quando a verificação de integridade falha.
- Você deve modificar os caminhos do diretório do log de auditoria e do diretório do log de soma de verificação de auditoria juntos. Você não pode modificar apenas um deles.
- Quando os caminhos do diretório do log de auditoria e do diretório do log de soma de verificação de auditoria são modificados, a verificação de integridade não pode ser executada nos logs de auditoria presentes no local anterior.
- Os caminhos do diretório do log de auditoria e do diretório do log de soma de verificação de auditoria devem estar na unidade local do SnapCenter Server.

  Unidades compartilhadas ou montadas em rede não são suportadas.

- Se o protocolo UDP for usado nas configurações do servidor Syslog, erros devido a porta inativa ou indisponível não poderão ser capturados como um erro ou um alerta no SnapCenter.
- Você pode usar os comandos Set-SmAuditSettings e Get-SmAuditSettings para configurar os logs de auditoria.

  As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando Get-Help command_name. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. Na página **Configurações**, navegue até **Configurações** > **Configurações globais** > **Configurações do log de auditoria**.

2. Na seção Log de auditoria, insira os detalhes.
3. Entre no **diretório de log de auditoria** e no **diretório de log de soma de verificação de auditoria**
   a. Digite o tamanho máximo do arquivo
   b. Insira o máximo de arquivos de log
   c. Insira a porcentagem de uso do espaço em disco para enviar um alerta
4. (Opcional) Habilite **Registrar hora UTC**.
5. (Opcional) Habilite **Agendamento de verificação de integridade do log de auditoria** e clique em **Iniciar verificação de integridade** para verificação de integridade sob demanda.

   Você também pode executar o comando **Start-SmAuditIntegrityCheck** para iniciar a verificação de integridade sob demanda.

6. (Opcional) Habilite Logs de auditoria encaminhados para o servidor syslog remoto e insira os detalhes do servidor syslog.

   Você deve importar o certificado do servidor Syslog para a 'Raiz Confiável' para o protocolo TLS 1.2.

   a. Digite o host do servidor Syslog
   b. Digite a porta do servidor Syslog
   c. Digite o protocolo do servidor Syslog
   d. Insira o formato RFC
7. Clique em **Salvar**.
8. Você pode ver as verificações de integridade de auditoria e as verificações de espaço em disco clicando em **Monitor** > **Tarefas**.

Configurar conexões MySQL seguras com o SnapCenter Server

Você pode gerar certificados Secure Sockets Layer (SSL) e arquivos de chave se quiser proteger a comunicação entre o SnapCenter Server e o MySQL Server em configurações autônomas ou configurações de balanceamento de carga de rede (NLB).

Configurar conexões MySQL seguras para configurações autônomas do SnapCenter Server

Você pode gerar certificados Secure Sockets Layer (SSL) e arquivos de chave se quiser proteger a comunicação entre o SnapCenter Server e o MySQL Server. Você deve configurar os certificados e arquivos de chave no MySQL Server e no SnapCenter Server.

Os seguintes certificados são gerados:

- Certificado CA
- Certificado público do servidor e arquivo de chave privada
- Certificado público do cliente e arquivo de chave privada

Passos

1. Configure os certificados SSL e os arquivos de chave para servidores e clientes MySQL no Windows usando o comando openssl.

Para obter informações, consulte "MySQL Versão 5.7: Criando Certificados e Chaves SSL Usando o OpenSSL"

> O valor do nome comum usado para o certificado do servidor, o certificado do cliente e os arquivos de chave deve ser diferente do valor do nome comum usado para o certificado da CA. Se os valores de nome comum forem os mesmos, os arquivos de certificado e chave falharão para servidores compilados usando OpenSSL.

Melhores práticas: você deve usar o nome de domínio totalmente qualificado (FQDN) do servidor como o nome comum para o certificado do servidor.

2. Copie os certificados SSL e os arquivos de chave para a pasta MySQL Data.

   O caminho padrão da pasta de dados do MySQL é `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

3. Atualize o certificado da CA, o certificado público do servidor, o certificado público do cliente, a chave privada do servidor e os caminhos da chave privada do cliente no arquivo de configuração do servidor MySQL (my.ini).

   O caminho padrão do arquivo de configuração do servidor MySQL (my.ini) é `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

   > Você deve especificar os caminhos do certificado CA, do certificado público do servidor e da chave privada do servidor na seção [mysqld] do arquivo de configuração do servidor MySQL (my.ini).

   Você deve especificar os caminhos do certificado CA, do certificado público do cliente e da chave privada do cliente na seção [cliente] do arquivo de configuração do servidor MySQL (my.ini).

   O exemplo a seguir mostra os certificados e arquivos de chave copiados para a seção [mysqld] do arquivo my.ini na pasta padrão `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"
```

   O exemplo a seguir mostra os caminhos atualizados na seção [client] do arquivo my.ini.

```
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. Pare o aplicativo Web SnapCenter Server no Internet Information Server (IIS).
5. Reinicie o serviço MySQL.
6. Atualize o valor da chave MySQLProtocol no arquivo SnapManager.Web.UI.dll.config.

   O exemplo a seguir mostra o valor da chave MySQLProtocol atualizada no arquivo SnapManager.Web.UI.dll.config.

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

7. Atualize o arquivo SnapManager.Web.UI.dll.config com os caminhos fornecidos na seção [client] do arquivo my.ini.

   O exemplo a seguir mostra os caminhos atualizados na seção [client] do arquivo my.ini.

```
<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. Inicie o aplicativo web SnapCenter Server no IIS.

Configurar conexões MySQL seguras para configurações de HA

Você pode gerar certificados Secure Sockets Layer (SSL) e arquivos de chave para os nós de Alta Disponibilidade (HA) se quiser proteger a comunicação entre o SnapCenter Server e os servidores MySQL. Você deve configurar os certificados e arquivos de chave nos servidores MySQL e nos nós HA.

Os seguintes certificados são gerados:

- Certificado CA

  Um certificado CA é gerado em um dos nós HA e esse certificado CA é copiado para o outro nó HA.

- Arquivos de certificado público do servidor e de chave privada do servidor para ambos os nós HA
- Arquivos de certificado público do cliente e de chave privada do cliente para ambos os nós HA

Passos

1. Para o primeiro nó HA, configure os certificados SSL e os arquivos de chave para servidores e clientes MySQL no Windows usando o comando openssl.

   Para obter informações, consulte "MySQL Versão 5.7: Criando Certificados e Chaves SSL Usando o OpenSSL"

   O valor do nome comum usado para o certificado do servidor, o certificado do cliente e os arquivos de chave deve ser diferente do valor do nome comum usado para o certificado da CA. Se os valores de nome comum forem os mesmos, os arquivos de certificado e chave falharão para servidores compilados usando OpenSSL.

   Melhores práticas: você deve usar o nome de domínio totalmente qualificado (FQDN) do servidor como o nome comum para o certificado do servidor.

2. Copie os certificados SSL e os arquivos de chave para a pasta MySQL Data.

   O caminho padrão da pasta de dados do MySQL é C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\.

3. Atualize o certificado da CA, o certificado público do servidor, o certificado público do cliente, a chave privada do servidor e os caminhos da chave privada do cliente no arquivo de configuração do servidor MySQL (my.ini).

   O caminho padrão do arquivo de configuração do servidor MySQL (my.ini) é C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\my.ini.

   Você deve especificar os caminhos do certificado CA, do certificado público do servidor e da chave privada do servidor na seção [mysqld] do arquivo de configuração do servidor MySQL (my.ini).

   Você deve especificar os caminhos do certificado CA, do certificado público do cliente e da chave privada do cliente na seção [cliente] do arquivo de configuração do servidor MySQL (my.ini).

   O exemplo a seguir mostra os certificados e arquivos de chave copiados para a seção [mysqld] do arquivo my.ini na pasta padrão 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"
```

O exemplo a seguir mostra os caminhos atualizados na seção [client] do arquivo my.ini.

```
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. Para o segundo nó HA, copie o certificado CA e gere o certificado público do servidor, os arquivos de chave privada do servidor, o certificado público do cliente e os arquivos de chave privada do cliente. Execute as seguintes etapas:

   a. Copie o certificado CA gerado no primeiro nó HA para a pasta MySQL Data do segundo nó NLB.

      O caminho padrão da pasta de dados do MySQL é C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\.

      > Você não deve criar um certificado de CA novamente. Você deve criar apenas o certificado público do servidor, o certificado público do cliente, o arquivo de chave privada do servidor e o arquivo de chave privada do cliente.

   b. Para o primeiro nó HA, configure os certificados SSL e os arquivos de chave para servidores e clientes MySQL no Windows usando o comando openssl.

      "MySQL Versão 5.7: Criando Certificados e Chaves SSL Usando o OpenSSL"

      > O valor do nome comum usado para o certificado do servidor, o certificado do cliente e os arquivos de chave deve ser diferente do valor do nome comum usado para o certificado da CA. Se os valores de nome comum forem os mesmos, os arquivos de certificado e chave falharão para servidores compilados usando OpenSSL.

      É recomendável usar o FQDN do servidor como o nome comum para o certificado do servidor.

   c. Copie os certificados SSL e os arquivos de chave para a pasta MySQL Data.

   d. Atualize o certificado da CA, o certificado público do servidor, o certificado público do cliente, a chave privada do servidor e os caminhos da chave privada do cliente no arquivo de configuração do servidor MySQL (my.ini).

Você deve especificar os caminhos do certificado CA, do certificado público do servidor e da chave privada do servidor na seção [mysqld] do arquivo de configuração do servidor MySQL (my.ini).

Você deve especificar os caminhos do certificado CA, do certificado público do cliente e da chave privada do cliente na seção [cliente] do arquivo de configuração do servidor MySQL (my.ini).

O exemplo a seguir mostra os certificados e arquivos de chave copiados para a seção [mysqld] do arquivo my.ini na pasta padrão 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"
```

O exemplo a seguir mostra os caminhos atualizados na seção [client] do arquivo my.ini.

```
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. Pare o aplicativo Web SnapCenter Server no Internet Information Server (IIS) em ambos os nós HA.
6. Reinicie o serviço MySQL em ambos os nós HA.
7. Atualize o valor da chave MySQLProtocol no arquivo SnapManager.Web.UI.dll.config para ambos os nós HA.

   O exemplo a seguir mostra o valor da chave MySQLProtocol atualizada no arquivo SnapManager.Web.UI.dll.config.

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

8. Atualize o arquivo SnapManager.Web.UI.dll.config com os caminhos que você especificou na seção [client] do arquivo my.ini para ambos os nós HA.

   O exemplo a seguir mostra os caminhos atualizados na seção [client] dos arquivos my.ini.

```
<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. Inicie o aplicativo Web SnapCenter Server no IIS em ambos os nós HA.
10. Use o cmdlet Set-SmRepositoryConfig -RebuildSlave -Force do PowerShell com a opção -Force em um dos nós HA para estabelecer a replicação segura do MySQL em ambos os nós HA.

    Mesmo que o status da replicação seja saudável, a opção -Force permite reconstruir o repositório escravo.

Configurar autenticação baseada em certificado

A autenticação baseada em certificado aumenta a segurança ao verificar a identidade do SnapCenter Server e dos hosts de plug-in, garantindo uma comunicação segura e criptografada.

Habilitar autenticação baseada em certificado

Para habilitar a autenticação baseada em certificado para o SnapCenter Server e os hosts de plug-in do Windows, execute o seguinte cmdlet do PowerShell. Para os hosts de plug-in do Linux, a autenticação baseada em certificado será habilitada quando você habilitar o SSL bidirecional.

- Para habilitar a autenticação baseada em certificado de cliente:

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- Para desabilitar a autenticação baseada em certificado de cliente:

```
Set-SmConfigSettings -Agent –configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

Exportar certificados de Autoridade Certificadora (CA) do SnapCenter Server

Você deve exportar os certificados de CA do SnapCenter Server para os hosts de plug-in usando o console de gerenciamento da Microsoft (MMC).

Antes de começar

Você deve ter configurado o SSL bidirecional.

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela Snap-in de Certificados, selecione a opção **Conta de Computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados - Computador local** > **Pessoal** > **Certificados**.
5. Clique com o botão direito do mouse no certificado CA adquirido, que é usado para o SnapCenter Server e selecione **Todas as tarefas** > **Exportar** para iniciar o assistente de exportação.
6. Execute as seguintes ações no assistente.

Para esta opção…	Faça o seguinte…
Exportar chave privada	Selecione **Não, não exportar a chave privada** e clique em **Avançar**.
Formato de arquivo de exportação	Clique em **Avançar**.
Nome do arquivo	Clique em **Procurar** e especifique o caminho do arquivo para salvar o certificado e clique em **Avançar**.
Concluindo o Assistente de Exportação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a exportação.

A autenticação baseada em certificado não é suportada para configurações do SnapCenter HA e do SnapCenter Plug-in for VMware vSphere.

Importar certificado CA para hosts de plug-in do Windows

Para usar o certificado CA do SnapCenter Server exportado, você deve importar o certificado relacionado para os hosts do plug-in do SnapCenter Windows usando o console de gerenciamento da Microsoft (MMC).

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela Snap-in de Certificados, selecione a opção **Conta de Computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados - Computador local** > **Pessoal** > **Certificados**.

5. Clique com o botão direito do mouse na pasta “Pessoal” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Execute as seguintes ações no assistente.

Para esta opção…	Faça o seguinte…
Localização da loja	Clique em **Avançar**.
Arquivo para importar	Selecione o certificado do SnapCenter Server que termina com a extensão .cer.
Loja de Certificados	Clique em **Avançar**.
Concluindo o Assistente de Exportação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

Importar certificado CA para hosts de plug-in UNIX

Você deve importar o certificado da CA para os hosts do plug-in UNIX.

Sobre esta tarefa

- Você pode gerenciar a senha do keystore SPL e o alias do par de chaves assinadas pela CA em uso.
- A senha para o keystore SPL e para todas as senhas de alias associadas da chave privada devem ser as mesmas.

Passos

1. Você pode recuperar a senha padrão do keystore SPL a partir do arquivo de propriedades SPL. É o valor correspondente à chave `SPL_KEYSTORE_PASS` .
2. Alterar a senha do keystore:
   `$ keytool -storepasswd -keystore keystore.jks`
3. Altere a senha de todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:
   `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. Atualize o mesmo para a chave SPL_KEYSTORE_PASS em `spl.properties` arquivo.
5. Reinicie o serviço após alterar a senha.

Configurar certificados raiz ou intermediários para armazenamento confiável SPL

Você deve configurar os certificados raiz ou intermediários para o armazenamento confiável SPL. Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Passos

1. Navegue até a pasta que contém o keystore SPL: `/var/opt/snapcenter/spl/etc` .
2. Localize o arquivo `keystore.jks` .
3. Listar os certificados adicionados no keystore:

```
$ keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:
```
$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported>
-file /<CertificatePath> -keystore keystore.jks
```

5. Reinicie o serviço após configurar os certificados raiz ou intermediários para o armazenamento confiável SPL.

Configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL

Você deve configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL.

Passos

1. Navegue até a pasta que contém o keystore do SPL `/var/opt/snapcenter/spl/etc` .
2. Localize o arquivo `keystore.jks` .
3. Listar os certificados adicionados no keystore:
```
$ keytool -list -v -keystore keystore.jks
```
4. Adicione o certificado da CA com chave privada e pública.
```
$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype
pkcs12 -destkeystore keystore.jks -deststoretype JKS
```
5. Listar os certificados adicionados no keystore.
```
$ keytool -list -v -keystore keystore.jks
```
6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

   A senha padrão do keystore SPL é o valor da chave SPL_KEYSTORE_PASS em `spl.properties` arquivo.

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks`
```

8. Se o nome do alias no certificado da CA for longo e contiver espaços ou caracteres especiais ("*",","), altere o nome do alias para um nome simples:
```
$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>"
-keystore keystore.jks`
```
9. Configure o nome do alias do keystore localizado em `spl.properties` arquivo. Atualize este valor em relação à chave SPL_CERTIFICATE_ALIAS.
10. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL.

Exportar certificados SnapCenter

Você deve exportar os certificados do SnapCenter no formato .pfx.

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover**

Snap-in.

2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Minha conta de usuário** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados - Usuário atual** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse no certificado que tem o Nome amigável do SnapCenter e selecione **Todas as tarefas** > **Exportar** para iniciar o assistente de exportação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Exportar chave privada	Selecione a opção **Sim, exportar a chave privada** e clique em **Avançar**.
Formato de arquivo de exportação	Não faça alterações; clique em **Avançar**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Arquivo para Exportar	Especifique um nome de arquivo para o certificado exportado (você deve usar .pfx) e clique em **Avançar**.
Concluindo o Assistente de Exportação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a exportação.

Configurar certificado CA para host Windows

Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.

O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte "Como gerar um arquivo CSR de certificado CA" .

Se você possui o certificado CA para seu domínio (*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host

devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Importar chave privada	Selecione a opção **Sim**, importe a chave privada e clique em **Avançar**.
Formato de arquivo de importação	Não faça alterações; clique em **Avançar**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

> O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: *.pfx, *.p12 e *.p7b).

7. Repita a Etapa 5 para a pasta “Pessoal”.

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

Passos

1. Execute o seguinte na GUI:
   a. Clique duas vezes no certificado.

b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.

c. Percorra a lista de campos e clique em **Impressão digital**.

d. Copie os caracteres hexadecimais da caixa.

e. Remova os espaços entre os números hexadecimais.

Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:

a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

Get-ChildItem -Path Cert:\LocalMachine\My

b. Copie a impressão digital.

Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

```
> netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
```

Por exemplo:

```
 > netsh http delete sslcert ipport=0.0.0.0:8145
. Vincule o certificado recém-instalado aos serviços de plug-in do host do Windows, executando os seguintes comandos:
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
```

Por exemplo:

```
> $cert = “a909502dd82ae41433e6f83886b00d4277a32a7b”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Configurar certificado CA com o site SnapCenter

Você deve configurar o certificado CA com o site SnapCenter no host Windows.

Passos

1. Abra o Gerenciador do IIS no Windows Server onde o SnapCenter está instalado.
2. No painel de navegação esquerdo, clique em **Conexões**.
3. Expanda o nome do servidor e **Sites**.
4. Selecione o site do SnapCenter no qual você deseja instalar o Certificado SSL.
5. Navegue até **Ações** > **Editar site** e clique em **Vinculações**.
6. Na página Ligações, selecione **ligação para https**.
7. Clique em **Editar**.
8. Na lista suspensa do certificado SSL, selecione o certificado SSL importado recentemente.
9. Clique em **OK**.

> O site do SnapCenter Scheduler (porta padrão: 8154, HTTPS) é configurado com certificado autoassinado. Esta porta está se comunicando dentro do host do SnapCenter Server e não é obrigatório configurá-la com um certificado CA. No entanto, se o seu ambiente exigir que você use um Certificado CA, repita as etapas 5 a 9 usando o site SnapCenter Scheduler.

> Se o certificado CA implantado recentemente não estiver listado no menu suspenso, verifique se o certificado CA está associado à chave privada.

> Certifique-se de que o certificado seja adicionado usando o seguinte caminho: **Raiz do console > Certificados – Computador local > Autoridades de certificação raiz confiáveis > Certificados**.

Habilitar certificados CA para SnapCenter

Você deve configurar os certificados CA e habilitar a validação do certificado CA para o SnapCenter Server.

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet Set-SmCertificateSettings.
- Você pode exibir o status do certificado do SnapCenter Server usando o cmdlet Get-SmCertificateSettings.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser

obtidas executando *Get-Help command_name*. Alternativamente, você pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. Na página Configurações, navegue até **Configurações** > **Configurações globais** > **Configurações do certificado CA**.
2. Selecione **Ativar validação de certificado**.
3. Clique em **Aplicar**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- * * indica que não há nenhum certificado CA habilitado ou atribuído ao host do plug-in.
- * * indica que o certificado CA foi validado com sucesso.
- * * indica que o certificado CA não pôde ser validado.
- * * indica que as informações de conexão não puderam ser recuperadas.

Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Configurar certificado CA para host Linux

Após instalar o SnapCenter Server no Linux, o instalador cria o certificado autoassinado. Se quiser usar o certificado CA, você deve configurar os certificados para o proxy reverso nginx, registro de auditoria e serviços do SnapCenter .

Configurar certificado nginx

Passos

1. Navegue até */etc/nginx/conf.d*: `cd /etc/nginx/conf.d`
2. Abra **snapcenter.conf** usando o vi ou qualquer editor de texto.
3. Navegue até a seção do servidor no arquivo de configuração.
4. Modifique os caminhos de *ssl_certificate* e *ssl_certificate_key* para apontar para o certificado CA.
5. Salve e feche o arquivo.
6. Recarregue o nginx: `$nginx -s reload`

Configurar certificado de log de auditoria

Passos

1. Abra *INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config* usando o vi ou qualquer editor de texto.

   O valor padrão de *INSTALL_DIR* é */opt*.

2. Edite as chaves **AUDILOG_CERTIFICATE_PATH** e **AUDILOG_CERTIFICATE_PASSWORD** para incluir o caminho do certificado CA e a senha, respectivamente.

   Somente o formato *.pfx* é suportado para certificado de log de auditoria.

3. Salve e feche o arquivo.
4. Reinicie o serviço **snapmanagerweb**: `$ systemctl restart snapmanagerweb`

Configurar certificado de serviços do SnapCenter

Passos

1. Abra os seguintes arquivos de configuração usando o vi ou qualquer editor de texto.
   - *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*

     O valor padrão de *INSTALL_DIR* é */opt*.

2. Edite as chaves **SERVICE_CERTIFICATE_PATH** e **SERVICE_CERTIFICATE_PASSWORD** para incluir o caminho do certificado da CA e a senha, respectivamente.

   Somente o formato *.pfx* é suportado para o certificado de serviços do SnapCenter .

3. Salve e feche os arquivos.
4. Reinicie todos os serviços.
   - `$ systemctl restart snapmanagerweb`
   - `$ systemctl restart smcore`
   - `$ systemctl restart scheduler`

Configurar e habilitar a comunicação SSL bidirecional no host Windows

Configurar comunicação SSL bidirecional no host Windows

Você deve configurar a comunicação SSL bidirecional para proteger a comunicação mútua entre o SnapCenter Server no host Windows e os plug-ins.

Antes de começar

- Você deve ter gerado o arquivo CSR do certificado CA com o comprimento mínimo de chave suportado de 3072.
- O certificado da CA deve oferecer suporte à autenticação do servidor e à autenticação do cliente.
- Você deve ter um certificado de CA com chave privada e detalhes de impressão digital.
- Você deve ter habilitado a configuração SSL unidirecional.

  Para mais detalhes, veja "Seção Configurar certificado CA."

- Você deve ter habilitado a comunicação SSL bidirecional em todos os hosts de plug-in e no SnapCenter Server.

  Ambientes com alguns hosts ou servidores não habilitados para comunicação SSL bidirecional não são suportados.

Passos

1. Para vincular a porta, execute as seguintes etapas no host do SnapCenter Server para a porta 8146 do servidor web SnapCenter IIS (padrão) e novamente para a porta 8145 do SMCore (padrão) usando comandos do PowerShell.

   a. Remova a vinculação de porta do certificado autoassinado existente do SnapCenter usando o seguinte comando do PowerShell.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
      ```

      Por exemplo,

      ```
      > netsh http delete sslcert ipport=0.0.0.0:8145

      > netsh http delete sslcert ipport=0.0.0.0:8146
      ```

   b. Vincule o certificado CA recém-adquirido ao servidor SnapCenter e à porta SMCore.

      ```
      > $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>
      ```

      Por exemplo,

      ```
      > $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. Para acessar a permissão para o certificado da CA, adicione o usuário do servidor web IIS padrão do SnapCenter "**IIS AppPool\ SnapCenter**" na lista de permissões de certificado executando as seguintes etapas para acessar o certificado da CA recém-adquirido.
   a. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover SnapIn**.
   b. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
   c. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
   d. Clique em **Console Root** > **Certificados – Computador local** > **Pessoal** > **Certificados**.
   e. Selecione o certificado SnapCenter .
   f. Para iniciar o assistente para adicionar usuário/permissão, clique com o botão direito do mouse no certificado da CA e selecione **Todas as tarefas** > **Gerenciar chaves privadas**.
   g. Clique em **Adicionar**, no assistente Selecionar usuários e grupos altere o local para o nome do computador local (o mais alto na hierarquia)
   h. Adicione o usuário IIS AppPool\ SnapCenter e conceda permissões de controle total.
3. Para **permissão do certificado CA IIS**, adicione a nova entrada de chaves de registro DWORD no SnapCenter Server a partir do seguinte caminho:

   No editor de registro do Windows, navegue até o caminho mencionado abaixo,

   ```
   HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv
   ders\SCHANNEL
   ```

4. Crie uma nova entrada de chave de registro DWORD no contexto da configuração do registro SCHANNEL.

   ```
   SendTrustedIssuerList = 0

   ClientAuthTrustMode = 2
   ```

Configurar o plug-in SnapCenter do Windows para comunicação SSL bidirecional

Você deve configurar o plug-in SnapCenter do Windows para comunicação SSL bidirecional usando comandos do PowerShell.

Antes de começar

Certifique-se de que a impressão digital do certificado da CA esteja disponível.

Passos

1. Para vincular a porta, execute as seguintes ações no host do plug-in do Windows para a porta 8145 do SMCore (padrão).
   a. Remova a vinculação de porta do certificado autoassinado existente do SnapCenter usando o seguinte comando do PowerShell.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
      ```

      Por exemplo,

      ```
      > netsh http delete sslcert ipport=0.0.0.0:8145
      ```

b. Vincule o certificado CA recém-adquirido à porta SMCore.

```
> $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>
```

Por exemplo,

```
> $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
```

Habilitar comunicação SSL bidirecional no host Windows

Você pode habilitar a comunicação SSL bidirecional para proteger a comunicação mútua entre o SnapCenter Server no host Windows e os plug-ins usando comandos do PowerShell.

Antes de começar

Execute os comandos para todos os plug-ins e o agente SMCore primeiro e depois para o servidor.

Passos

1. Para habilitar a comunicação SSL bidirecional, execute os seguintes comandos no SnapCenter Server para os plug-ins, o servidor e para cada um dos agentes para os quais a comunicação SSL bidirecional é necessária.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. Execute a operação de reciclagem do pool de aplicativos do IIS SnapCenter usando o seguinte comando.
   `> Restart-WebAppPool -Name "SnapCenter"`
3. Para plug-ins do Windows, reinicie o serviço SMCore executando o seguinte comando do PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

Desabilitar comunicação SSL bidirecional

Você pode desabilitar a comunicação SSL bidirecional usando comandos do PowerShell.

Sobre esta tarefa

- Execute os comandos para todos os plug-ins e o agente SMCore primeiro e depois para o servidor.
- Quando você desabilita a comunicação SSL bidirecional, o certificado da CA e sua configuração não são removidos.
- Para adicionar um novo host ao SnapCenter Server, você deve desabilitar o SSL bidirecional para todos os hosts de plug-in.
- NLB e F5 não são suportados.

Passos

1. Para desabilitar a comunicação SSL bidirecional, execute os seguintes comandos no SnapCenter Server para todos os hosts de plug-in e o host SnapCenter .

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName <Agent_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. Execute a operação de reciclagem do pool de aplicativos do IIS SnapCenter usando o seguinte comando.
```
> Restart-WebAppPool -Name "SnapCenter"
```
3. Para plug-ins do Windows, reinicie o serviço SMCore executando o seguinte comando do PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

Configurar e habilitar comunicação SSL bidirecional no host Linux

Configurar comunicação SSL bidirecional no host Linux

Você deve configurar a comunicação SSL bidirecional para proteger a comunicação mútua entre o SnapCenter Server no host Linux e os plug-ins.

Antes de começar

- Você deve ter configurado o certificado CA para o host Linux.
- Você deve ter habilitado a comunicação SSL bidirecional em todos os hosts de plug-in e no SnapCenter Server.

Passos

1. Copie **certificate.pem** para */etc/pki/ca-trust/source/anchors/*.
2. Adicione os certificados na lista de confiança do seu host Linux.
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. Verifique se os certificados foram adicionados à lista de confiança.
   `trust list | grep "<CN of your certificate>"`
4. Atualize **ssl_certificate** e **ssl_certificate_key** no arquivo SnapCenter **nginx** e reinicie.
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. Atualize o link da GUI do SnapCenter Server.
6. Atualize os valores das seguintes chaves em * SnapManager.Web.UI.dll.config* localizado em _ /<caminho de instalação>/ NetApp/snapcenter/SnapManagerWeb_ e **SMCoreServiceHost.dll.config** localizado em */<caminho de instalação>/ NetApp/snapcenter/SMCore*.
   - <add key="SERVICE_CERTIFICATE_PATH" value="<caminho do certificado.pfx>" />
   - <adicionar chave="SENHA_DO_CERTIFICADO_DE_SERVIÇO" valor="<senha>"/>
7. Reinicie os seguintes serviços.
   - `systemctl restart smcore.service`
   - `systemctl restart snapmanagerweb.service`
8. Verifique se o certificado está anexado à porta da web do SnapManager .
   `openssl s_client -connect localhost:8146 -brief`
9. Verifique se o certificado está anexado à porta smcore.
   `openssl s_client -connect localhost:8145 -brief`
10. Gerenciar senha para keystore e alias SPL.
    a. Recupere a senha padrão do keystore SPL atribuída à chave **SPL_KEYSTORE_PASS** no arquivo de propriedades SPL.
    b. Alterar a senha do keystore.
       `keytool -storepasswd -keystore keystore.jks`
    c. Altere a senha de todos os aliases de entradas de chave privada.
       `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
    d. Atualize a mesma senha para a chave **SPL_KEYSTORE_PASS** em *spl.properties*.
    e. Reinicie o serviço.
11. No host Linux do plug-in, adicione os certificados raiz e intermediário no keystore do plug-in SPL.
    - `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. Verifique as entradas em keystore.jks.
`keytool -list -v -keystore <path to keystore.jks>`

ii. Renomeie qualquer alias, se necessário.
`keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`

12. Atualize o valor de **SPL_CERTIFICATE_ALIAS** no arquivo *spl.properties* com o alias de **certificate.pfx** armazenado em *keystore.jks* e reinicie o serviço SPL: `systemctl restart spl`

13. Verifique se o certificado está anexado à porta smcore.
`openssl s_client -connect localhost:8145 -brief`

Habilitar comunicação SSL no host Linux

Você pode habilitar a comunicação SSL bidirecional para proteger a comunicação mútua entre o SnapCenter Server no host Linux e os plug-ins usando comandos do PowerShell.

Etapa

1. Execute o seguinte para habilitar a comunicação SSL unidirecional.
   a. Efetue login na interface gráfica do usuário do SnapCenter .
   b. Clique em **Configurações** > **Configurações globais** e selecione **Ativar validação de certificado no SnapCenter Server**.
   c. Clique em **Hosts** > **Hosts gerenciados** e selecione o host do plug-in para o qual você deseja habilitar o SSL unidirecional.
   d. Clique ícone e clique em **Ativar validação de certificado**.
2. Habilite a comunicação SSL bidirecional do host Linux do SnapCenter Server.
   - `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"}`

Configurar Active Directory, LDAP e LDAPS

Registrar domínios não confiáveis do Active Directory

Você deve registrar o Active Directory com o SnapCenter Server para gerenciar hosts, usuários e grupos de vários domínios não confiáveis do Active Directory.

Antes de começar

Protocolos LDAP e LDAPS

- Você pode registrar domínios não confiáveis do Active Directory usando o protocolo LDAP ou LDAPS.
- Você deve ter habilitado a comunicação bidirecional entre os hosts do plug-in e o SnapCenter Server.

- A resolução de DNS deve ser configurada do SnapCenter Server para os hosts de plug-in e vice-versa.

Protocolo LDAP

- O nome de domínio totalmente qualificado (FQDN) deve ser resolvível no SnapCenter Server.

  Você pode registrar um domínio não confiável com o FQDN. Se o FQDN não puder ser resolvido no SnapCenter Server, você poderá registrar com um endereço IP de controlador de domínio, e isso poderá ser resolvido no SnapCenter Server.

Protocolo LDAPS

- Os certificados CA são necessários para que o LDAPS forneça criptografia de ponta a ponta durante a comunicação do diretório ativo.

  "Configurar certificado de cliente CA para LDAPS"

- Os nomes de host do controlador de domínio (DCHostName) devem ser acessíveis pelo SnapCenter Server.

Sobre esta tarefa

- Você pode usar a interface de usuário do SnapCenter , os cmdlets do PowerShell ou a API REST para registrar um domínio não confiável.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Configurações globais**.
3. Na página Configurações globais, clique em **Configurações de domínio**.
4. Clique + para registrar um novo domínio.
5. Na página Registrar novo domínio, selecione **LDAP** ou **LDAPS**.
   a. Se você selecionar **LDAP**, especifique as informações necessárias para registrar o domínio não confiável para LDAP:

Para este campo…	Faça isso…
Nome de domínio	Especifique o nome NetBIOS para o domínio.
FQDN de domínio	Especifique o FQDN e clique em **Resolver**.
Endereços IP do controlador de domínio	Se o FQDN do domínio não puder ser resolvido no SnapCenter Server, especifique um ou mais endereços IP do controlador de domínio. Para obter mais informações, consulte "Adicionar IP do controlador de domínio para domínio não confiável da GUI" .

   b. Se você selecionar **LDAPS**, especifique as informações necessárias para registrar o domínio não

confiável para LDAPS:

Para este campo…	Faça isso…
Nome de domínio	Especifique o nome NetBIOS para o domínio.
FQDN de domínio	Especifique o FQDN.
Nomes de controladores de domínio	Especifique um ou mais nomes de controladores de domínio e clique em **Resolver**.
Endereços IP do controlador de domínio	Se os nomes dos controladores de domínio não puderem ser resolvidos pelo SnapCenter Server, você deverá retificar as resoluções de DNS.

6. Clique em **OK**.

Configurar pools de aplicativos do IIS para habilitar permissões de leitura do Active Directory

Você pode configurar o Internet Information Services (IIS) no seu Windows Server para criar uma conta personalizada do Application Pool quando precisar habilitar permissões de leitura do Active Directory para o SnapCenter.

Passos

1. Abra o Gerenciador do IIS no Windows Server onde o SnapCenter está instalado.
2. No painel de navegação esquerdo, clique em **Pools de aplicativos**.
3. Selecione SnapCenter na lista Pools de aplicativos e clique em **Configurações avançadas** no painel Ações.
4. Selecione Identidade e clique em **…** para editar a identidade do pool de aplicativos do SnapCenter .
5. No campo Conta personalizada, insira um nome de conta de usuário ou administrador de domínio com permissão de leitura do Active Directory.
6. Clique em OK.

   A conta personalizada substitui a conta ApplicationPoolIdentity interna para o pool de aplicativos SnapCenter .

Configurar certificado de cliente CA para LDAPS

Você deve configurar o certificado do cliente CA para LDAPS no SnapCenter Server quando o Windows Active Directory LDAPS estiver configurado com os certificados CA.

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.

3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	**Faça o seguinte…**
Na segunda página do assistente	Clique em **Procurar**, selecione o *Certificado Raiz* e clique em **Avançar**.
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

7. Repita as etapas 5 e 6 para os certificados intermediários.

Proteja bancos de dados do Microsoft SQL Server

Plug-in SnapCenter para Microsoft SQL Server

Visão geral do plug-in SnapCenter para Microsoft SQL Server

O SnapCenter Plug-in para Microsoft SQL Server é um componente do lado do host do NetApp SnapCenter Software que permite o gerenciamento de proteção de dados com reconhecimento de aplicativo de bancos de dados do Microsoft SQL Server. O plug-in para SQL Server automatiza as operações de backup, verificação, restauração e clonagem do banco de dados SQL Server no seu ambiente SnapCenter .

Quando o Plug-in para SQL Server estiver instalado, você poderá usar o SnapCenter com a tecnologia NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia NetApp SnapVault para executar a replicação de backup de disco para disco para fins de conformidade com padrões ou arquivamento.

- Automatiza operações de backup, restauração e clonagem com reconhecimento de aplicativo para bancos de dados Microsoft SQL Server no seu ambiente SnapCenter .
- Oferece suporte a bancos de dados Microsoft SQL Server em VMDK e LUNs de mapeamento de dispositivos brutos (RDM) quando você implanta o SnapCenter Plug-in for VMware vSphere e registra o plug-in com o SnapCenter
- Suporta somente o provisionamento de compartilhamentos SMB. Não há suporte para backup de bancos de dados SQL Server em compartilhamentos SMB.
- Suporta a importação de backups do SnapManager para Microsoft SQL Server para o SnapCenter.

O que você pode fazer com o plug-in SnapCenter para Microsoft SQL Server

Quando o SnapCenter Plug-in para Microsoft SQL Server estiver instalado em seu ambiente, você poderá usar o SnapCenter para fazer backup, restaurar e clonar bancos de dados do SQL Server.

Você pode executar as seguintes tarefas que dão suporte a operações de backup, operações de restauração e operações de clonagem de bancos de dados e recursos de banco de dados do SQL Server:

- Faça backup de bancos de dados do SQL Server e logs de transações associados

  Não é possível criar um backup de log para bancos de dados do sistema master e msdb. No entanto, você pode criar backups de log para o banco de dados do sistema modelo.

- Restaurar recursos do banco de dados
  - Você pode restaurar bancos de dados do sistema mestre, bancos de dados do sistema msdb e bancos de dados do sistema modelo.
  - Não é possível restaurar vários bancos de dados, instâncias e grupos de disponibilidade.
  - Não é possível restaurar o banco de dados do sistema para um caminho alternativo.
- Crie clones pontuais de bancos de dados de produção

Não é possível executar operações de backup, restauração, clonagem e ciclo de vida de clonagem em bancos de dados do sistema tempdb.

- Verifique as operações de backup imediatamente ou adie a verificação para mais tarde

  A verificação do banco de dados do sistema SQL Server não é suportada. O SnapCenter clona os bancos de dados para executar a operação de verificação. O SnapCenter não pode clonar bancos de dados do sistema SQL Server e, portanto, a verificação desses bancos de dados não é suportada.

- Agendar operações de backup e operações de clonagem
- Monitorar operações de backup, operações de restauração e operações de clonagem

O plug-in para SQL Server não oferece suporte a backup e recuperação de bancos de dados SQL Server em compartilhamentos SMB.

Recursos do plug-in SnapCenter para Microsoft SQL Server

O plug-in para SQL Server integra-se ao Microsoft SQL Server no host Windows e à tecnologia NetApp Snapshot no sistema de armazenamento. Para trabalhar com o Plug-in para SQL Server, use a interface do SnapCenter .

O plug-in para SQL Server inclui estes recursos principais:

- **Interface gráfica de usuário unificada com tecnologia SnapCenter**

  A interface do SnapCenter oferece padronização e consistência entre plug-ins e ambientes. A interface do SnapCenter permite que você conclua processos consistentes de backup e restauração em todos os plug-ins, use relatórios centralizados, use visualizações de painel rápidas, configure o controle de acesso baseado em função (RBAC) e monitore trabalhos em todos os plug-ins. O SnapCenter também oferece agendamento centralizado e gerenciamento de políticas para dar suporte a operações de backup e clonagem.

- **Administração central automatizada**

  Você pode agendar backups de rotina do SQL Server, configurar retenção de backup baseada em políticas e configurar operações de restauração atualizadas e em tempo real. Você também pode monitorar proativamente seu ambiente do SQL Server configurando o SnapCenter para enviar alertas por e-mail.

- **Tecnologia NetApp Snapshot não disruptiva**

  O plug-in para SQL Server usa a tecnologia NetApp Snapshot com o plug-in NetApp SnapCenter para Microsoft Windows. Isso permite que você faça backup de bancos de dados em segundos e restaure-os rapidamente sem deixar o SQL Server offline. Os instantâneos consomem espaço de armazenamento mínimo.

Além desses recursos principais, o Plug-in para SQL Server oferece os seguintes benefícios:

- Suporte ao fluxo de trabalho de backup, restauração, clonagem e verificação
- Segurança com suporte RBAC e delegação centralizada de funções
- Criação de cópias pontuais e com economia de espaço de bancos de dados de produção para testes ou extração de dados usando a tecnologia NetApp FlexClone

Uma licença FlexClone é necessária no sistema de armazenamento que contém o clone.

- Verificação de backup automatizada e sem interrupções
- Capacidade de executar vários backups ao mesmo tempo em vários servidores
- Cmdlets do PowerShell para scripts de operações de backup, verificação, restauração e clonagem
- Suporte para Grupos de Disponibilidade AlwaysOn (AGs) no SQL Server para acelerar as operações de configuração, backup e restauração do AG
- Banco de dados na memória e extensão de pool de buffer (BPE) como parte do SQL Server 2014
- Suporte para backup de LUNs e discos de máquinas virtuais (VMDKs)
- Suporte para infraestruturas físicas e virtualizadas
- Suporte para iSCSI, Fibre Channel, FCoE, mapeamento de dispositivos brutos (RDM) e VMDK sobre NFS e VMFS

  Os volumes NAS devem ter uma política de exportação padrão na máquina virtual de armazenamento (SVM).

- Suporte para FileStream e grupo de arquivos em bancos de dados independentes do SQL Server.
- Suporte para memória não volátil expressa (NVMe) no Windows Server 2022
  - Fluxos de trabalho de backup, restauração, clonagem e verificação no layout VMDK criado em NVMe sobre TCP/IP.
  - Suporta firmware NVMe versão 1.3 a partir do ESX 8.0 atualização 2 e requer hardware virtual versão 21.
  - O Windows Server Failover Clustering (WSFC) não é suportado para aplicativos via VMDK em NVMe via TCP/IP.
- Oferece suporte à sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC]), que permite que os serviços empresariais continuem operando mesmo durante uma falha completa do site, permitindo que os aplicativos façam failover de forma transparente usando uma cópia secundária. Não é necessária intervenção manual nem script adicional para acionar um failover com a sincronização ativa do SnapMirror .

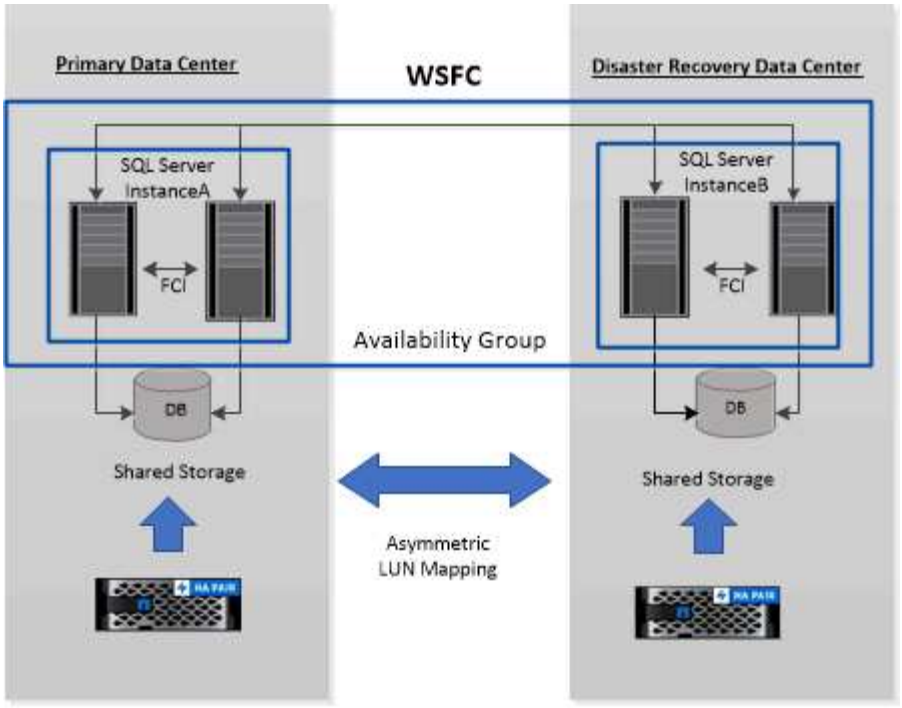
Suporte para mapeamento assimétrico de LUN em clusters do Windows

O plug-in SnapCenter para Microsoft SQL Server oferece suporte à descoberta no SQL Server 2012 e versões posteriores, configurações de mapeamento de LUN assimétrico (ALM) para alta disponibilidade e grupos de disponibilidade para recuperação de desastres. Ao descobrir recursos, o SnapCenter descobre bancos de dados em hosts locais e em hosts remotos em configurações do ALM.

Uma configuração ALM é um único cluster de failover de servidor Windows que contém um ou mais nós em um data center primário e um ou mais nós em um centro de recuperação de desastres.

A seguir está um exemplo de uma configuração de ALM:

- Duas instâncias de cluster de failover (FCI) em um datacenter multisite
- FCI para alta disponibilidade local (HA) e Grupo de Disponibilidade (AG) para recuperação de desastres com uma instância autônoma no local de recuperação de desastres



WSFC----Windows Server Failover Cluster

O armazenamento no datacenter primário é compartilhado entre os nós FCI presentes no datacenter primário. O armazenamento no datacenter de recuperação de desastres é compartilhado entre os nós FCI presentes no datacenter de recuperação de desastres.

O armazenamento no datacenter principal não é visível para os nós no datacenter de recuperação de desastres e vice-versa.

A arquitetura ALM combina duas soluções de armazenamento compartilhado usadas pela FCI, com uma solução de armazenamento não compartilhado ou dedicado usada pela SQL AG. A solução AG usa letras de unidade idênticas para recursos de disco compartilhados entre data centers. Esse arranjo de armazenamento, em que um disco de cluster é compartilhado entre um subconjunto de nós dentro de um WSFC, é chamado de ALM.

Tipos de armazenamento suportados pelo SnapCenter Plug-in para Microsoft SQL Server

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e virtuais. Você deve verificar se o suporte está disponível para seu tipo de armazenamento antes de instalar o pacote para seu host.

O suporte ao provisionamento e à proteção de dados do SnapCenter está disponível no Windows Server. Para obter as informações mais recentes sobre as versões suportadas, consulte ohttps://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT["Ferramenta de Matriz de Interoperabilidade da NetApp"^] .

Máquina	Tipo de armazenamento	Provisão usando	Notas de suporte
Servidor físico	LUNs conectados por FC	Interface gráfica do usuário (GUI) do SnapCenter ou cmdlets do PowerShell	
Servidor físico	LUNs conectados por iSCSI	Cmdlets do SnapCenter GUI ou PowerShell	
Servidor físico	Compartilhamentos SMB3 (CIFS) residindo em uma máquina virtual de armazenamento (SVM)	Cmdlets do SnapCenter GUI ou PowerShell	Suporte somente para provisionamento.
VMware VM	LUNs RDM conectados por um FC ou iSCSI HBA	Cmdlets do PowerShell	
VMware VM	LUNs iSCSI conectados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets do SnapCenter GUI ou PowerShell	
VMware VM	Sistemas de arquivos de máquina virtual (VMFS) ou armazenamentos de dados NFS	VMware vSphere	
VMware VM	Um sistema convidado conectado a compartilhamentos SMB3 que residem em um SVM	Cmdlets do SnapCenter GUI ou PowerShell	Suporte somente para provisionamento.
VMware VM	Armazenamentos de dados vVol em NFS e SAN	Ferramentas ONTAP para VMware vSphere	

Máquina	Tipo de armazenamento	Provisão usando	Notas de suporte
VM Hyper-V	LUNs FC virtuais (vFC) conectados por um switch Fibre Channel virtual	Cmdlets do SnapCenter GUI ou PowerShell	Você deve usar o Hyper-V Manager para provisionar LUNs de FC Virtual (vFC) conectados por um Switch de Canal de Fibra virtual. Não há suporte para discos de passagem do Hyper-V e backup de bancos de dados em VHD(x) provisionados no armazenamento NetApp .
VM Hyper-V	LUNs iSCSI conectados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets do SnapCenter GUI ou PowerShell	Não há suporte para discos de passagem do Hyper-V e backup de bancos de dados em VHD(x) provisionados no armazenamento NetApp .

Máquina	Tipo de armazenamento	Provisão usando	Notas de suporte
VM Hyper-V	Um sistema convidado conectado a compartilhamentos SMB3 que residem em um SVM	Cmdlets do SnapCenter GUI ou PowerShell	Suporte somente para provisionamento. Não há suporte para discos de passagem do Hyper-V e backup de bancos de dados em VHD(x) provisionados no armazenamento NetApp .

Recomendações de layout de armazenamento para o plug-in SnapCenter para Microsoft SQL Server

Um layout de armazenamento bem projetado permite que o SnapCenter Server faça backup de seus bancos de dados para atender aos seus objetivos de recuperação. Você deve considerar vários fatores ao definir seu layout de armazenamento, incluindo o tamanho do banco de dados, a taxa de alteração do banco de dados e a frequência com que você realiza backups.

As seções a seguir definem as recomendações e restrições de layout de armazenamento para LUNs e discos de máquina virtual (VMDKs) com o SnapCenter Plug-in para Microsoft SQL Server instalado em seu ambiente.

Nesse caso, os LUNs podem incluir discos VMware RDM e LUNs iSCSI conectados diretamente que são mapeados para o convidado.

Requisitos de LUN e VMDK

Opcionalmente, você pode usar LUNs ou VMDKs dedicados para obter desempenho e gerenciamento ideais para os seguintes bancos de dados:

- Bancos de dados de sistemas mestre e modelo
- Banco de dados temporário
- Arquivos de banco de dados do usuário (.mdf e .ndf)
- Arquivos de log de transações do banco de dados do usuário (.ldf)
- Diretório de log

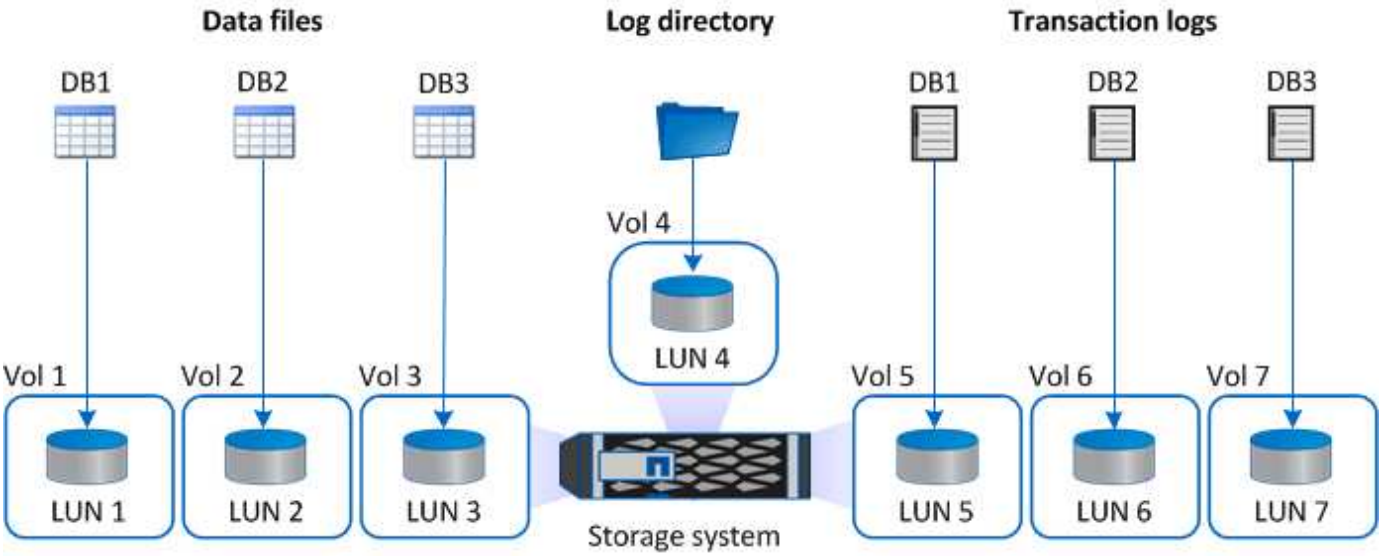
Para restaurar grandes bancos de dados, a melhor prática é usar LUNs ou VMDKs dedicados. O tempo necessário para restaurar um LUN ou VMDK completo é menor que o tempo necessário para restaurar os

arquivos individuais armazenados no LUN ou VMDK.

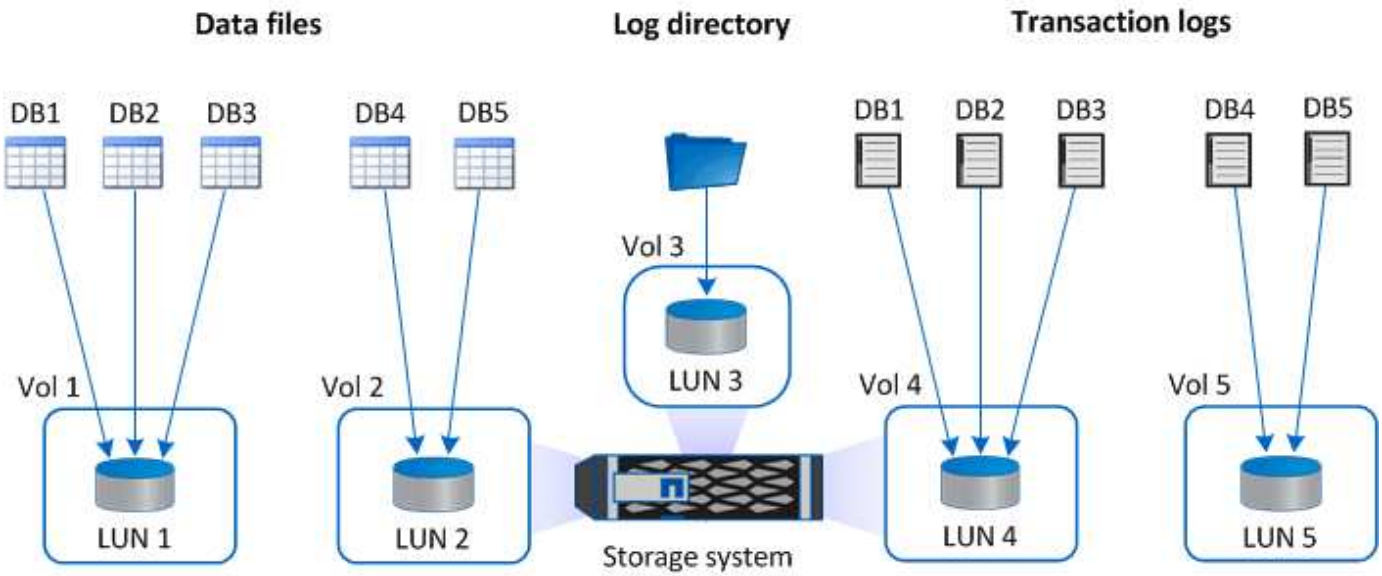
Para o diretório de log, você deve criar um LUN ou VMDK separado para que haja espaço livre suficiente nos discos de dados ou arquivos de log.

Layouts de amostra de LUN e VMDK

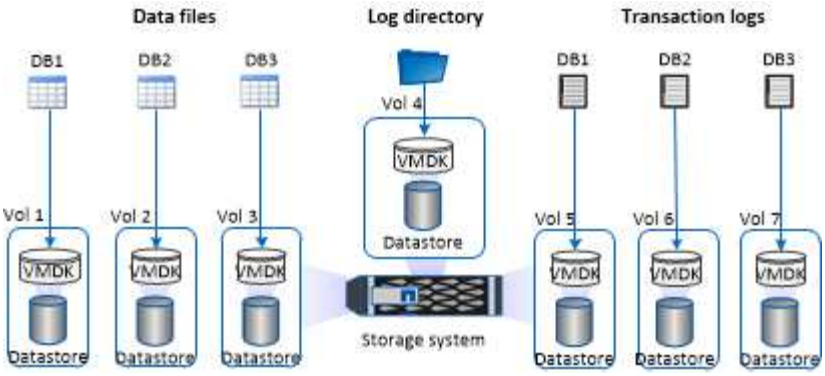
O gráfico a seguir mostra como você pode configurar o layout de armazenamento para grandes bancos de dados em LUNs:



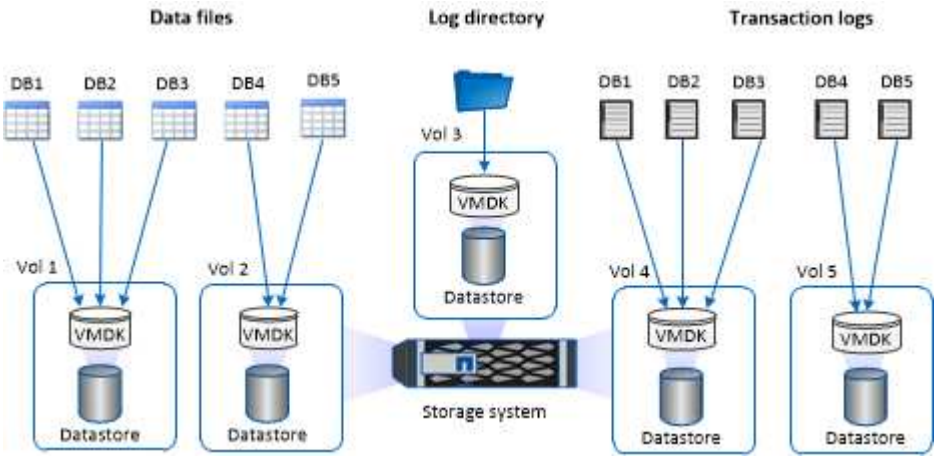
O gráfico a seguir mostra como você pode configurar o layout de armazenamento para bancos de dados médios ou pequenos em LUNs:



O gráfico a seguir mostra como você pode configurar o layout de armazenamento para grandes bancos de dados em VMDKs:



O gráfico a seguir mostra como você pode configurar o layout de armazenamento para bancos de dados médios ou pequenos em VMDKs:



Privilégios ONTAP mínimos necessários para o plug-in SQL

Os privilégios mínimos do ONTAP necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos de acesso total: privilégios mínimos necessários para ONTAP 9.12.1 e posterior
  - evento generate-autosupport-log
  - histórico de trabalho mostrar
  - parada de trabalho
  - lua
  - lun criar
  - lun delete
  - lun igroup adicionar
  - lun igroup criar
  - lun igroup excluir
  - renomear lun igroup
  - show do lun igroup
  - mapeamento lun add-reporting-nodes
  - criação de mapeamento lun

- exclusão de mapeamento lun
- mapeamento lun remove-reporting-nodes
- show de mapeamento lunar
- lun modificar
- volume de entrada lun
- lua offline
- lua online
- redimensionamento de lun
- série lun
- show de lua
- política de adição de regra do snapmirror
- regra de modificação de política do snapmirror
- política de remoção do snapmirror
- política do snapmirror mostrar
- restauração do snapmirror
- show de espelhos instantâneos
- histórico de exibição do snapmirror
- atualização do snapmirror
- atualização do snapmirror-ls-set
- lista-destinos do snapmirror
- versão
- criação de clone de volume
- show de clones de volume
- volume clone split start
- volume clone divisão parada
- volume criar
- destruição de volume
- clone de arquivo de volume criar
- arquivo de volume mostrar-uso-do-disco
- volume offline
- volume on-line
- modificação de volume
- volume qtree criar
- volume qtree delete
- volume qtree modificar
- volume qtree mostrar
- restrição de volume

- show de volume
- criação de instantâneo de volume
- exclusão de instantâneo de volume
- modificação de instantâneo de volume
- renomeação de instantâneo de volume
- restauração de instantâneo de volume
- arquivo de restauração de instantâneo de volume
- exibição de instantâneo de volume
- desmontagem de volume
- cifs do vserver
- vserver cifs compartilhar criar
- vserver cifs compartilhar excluir
- vserver cifs shadowcopy mostrar
- vserver cifs compartilhar mostrar
- vserver cifs mostrar
- política de exportação do vserver
- criação de política de exportação do vserver
- exclusão da política de exportação do vserver
- criação de regra de política de exportação do vserver
- mostrar regra de política de exportação do vserver
- mostrar política de exportação do vserver
- vserver iscsi
- mostrar conexão iscsi do vserver
- vserver mostrar
- interface de rede
- exibição de interface de rede
- vserver
- show do metrocluster

Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para Plug-in para servidor SQL

Você pode usar um plug-in SnapCenter com a tecnologia ONTAP SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia ONTAP SnapVault para executar replicação de backup de disco para disco para conformidade com padrões e outros propósitos relacionados à governança. Antes de executar essas tarefas, você deve configurar um relacionamento de proteção de dados entre os volumes de origem e destino e inicializar o relacionamento.

O SnapCenter executa as atualizações no SnapMirror e no SnapVault após concluir a operação Snapshot. As

atualizações do SnapMirror e do SnapVault são executadas como parte do trabalho do SnapCenter ; não crie uma programação ONTAP separada.

> Se você estiver acessando o SnapCenter a partir de um produto NetApp SnapManager e estiver satisfeito com os relacionamentos de proteção de dados configurados, pode pular esta seção.

Um relacionamento de proteção de dados replica dados do armazenamento primário (o volume de origem) para o armazenamento secundário (o volume de destino). Quando você inicializa o relacionamento, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

> O SnapCenter não oferece suporte a relacionamentos em cascata entre volumes SnapMirror e SnapVault (**Primário** > **Espelho** > **Cofre**). Você deve usar relacionamentos fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis em termos de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis em termos de versão e como configurá-los, consulte "Documentação do ONTAP" .

Estratégia de backup para recursos do SQL Server

Definir uma estratégia de backup para recursos do SQL Server

Definir uma estratégia de backup antes de criar suas tarefas de backup ajuda a garantir que você tenha os backups necessários para restaurar ou clonar seus bancos de dados com sucesso. Seu Contrato de Nível de Serviço (SLA), Objetivo de Tempo de Recuperação (RTO) e Objetivo de Ponto de Recuperação (RPO) determinam em grande parte sua estratégia de backup.

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. O RTO é o momento em que um processo de negócios deve ser restaurado após uma interrupção no serviço. Um RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. O SLA, o RTO e o RPO contribuem para a estratégia de backup.

Tipo de backups suportados

Para fazer backup do sistema SQL Server e dos bancos de dados do usuário usando o SnapCenter , é necessário escolher o tipo de recurso, como bancos de dados, instâncias do SQL Server e Grupos de Disponibilidade (AG). A tecnologia de instantâneo é utilizada para criar cópias on-line, somente leitura, dos volumes nos quais os recursos residem.

Você pode selecionar a opção somente cópia para especificar que o SQL Server não trunque os logs de transações. Você deve usar esta opção quando também estiver gerenciando o SQL Server com outros aplicativos de backup. Manter os logs de transações intactos permite que qualquer aplicativo de backup restaure os bancos de dados do sistema. Os backups somente cópia são independentes da sequência de backups agendados e não afetam os procedimentos de backup e restauração do banco de dados.

Tipo de backup	Descrição	Opção somente cópia com tipo de backup
Backup completo e backup de log	Faz backup do banco de dados do sistema e trunca os logs de transações. O SQL Server trunca os logs de transações removendo as entradas que já estão confirmadas no banco de dados. Após a conclusão do backup completo, esta opção cria um log de transações que captura informações da transação. Normalmente, você deve escolher esta opção. No entanto, se o tempo de backup for curto, você pode optar por não executar um backup de log de transações com backup completo. Não é possível criar um backup de log para bancos de dados do sistema master e msdb. No entanto, você pode criar backups de log para o banco de dados do sistema modelo.	Faz backup dos arquivos de banco de dados do sistema e dos logs de transações sem truncar os logs. Um backup somente cópia não pode servir como base diferencial ou backup diferencial e não afeta a base diferencial. Restaurar um backup completo somente cópia é o mesmo que restaurar qualquer outro backup completo.
Backup completo do banco de dados	Faz backup dos arquivos de banco de dados do sistema. Você pode criar um backup completo do banco de dados para bancos de dados do sistema mestre, modelo e msdb.	Faz backup dos arquivos de banco de dados do sistema.
Backup do log de transações	Faz backup dos logs de transações truncados, copiando apenas as transações que foram confirmadas desde que o log de transações mais recente foi feito backup. Se você agendar backups frequentes de log de transações junto com backups completos do banco de dados, poderá escolher pontos de recuperação granulares.	Faz backup dos logs de transações sem truncá-los. Este tipo de backup não afeta o sequenciamento de backups de log regulares. Backups de log somente cópia são úteis para executar operações de restauração on-line.

Agendamentos de backup para plug-in para servidor SQL

A frequência de backup (tipo de agendamento) é especificada nas políticas; um agendamento de backup é especificado na configuração do grupo de recursos. O fator mais crítico na determinação da frequência ou programação de backup é a taxa de alteração do recurso e a importância dos dados. Você pode fazer backup de um recurso muito utilizado a cada hora, enquanto pode fazer backup de um recurso raramente utilizado uma vez por dia. Outros fatores incluem a importância do recurso para sua organização, seu Acordo de Nível de Serviço (SLA) e seu Objetivo de Ponto de Recuperação (RPO).

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. Um RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. O SLA e o RPO contribuem para a estratégia de proteção de dados.

Mesmo para um recurso muito utilizado, não há necessidade de executar um backup completo mais de uma ou duas vezes por dia. Por exemplo, backups regulares do log de transações podem ser suficientes para garantir que você tenha os backups necessários. Quanto mais você fizer backup dos seus bancos de dados, menos logs de transações o SnapCenter terá que usar no momento da restauração, o que pode resultar em operações de restauração mais rápidas.

Os agendamentos de backup têm duas partes, conforme a seguir:

- Frequência de backup

  A frequência de backup (com que frequência os backups devem ser realizados), chamada de *tipo de agendamento* para alguns plug-ins, faz parte de uma configuração de política. Você pode selecionar por hora, dia, semana ou mês como a frequência de backup da política. Se você não selecionar nenhuma dessas frequências, a política criada será somente sob demanda. Você pode acessar as políticas clicando em **Configurações** > **Políticas**.

- Agendamentos de backup

  Os agendamentos de backup (exatamente quando os backups devem ser executados) fazem parte de uma configuração de grupo de recursos. Por exemplo, se você tiver um grupo de recursos com uma política configurada para backups semanais, poderá configurar o agendamento para fazer backup toda quinta-feira às 22h. Você pode acessar as programações dos grupos de recursos clicando em **Recursos** > **Grupos de Recursos**.

Número de trabalhos de backup necessários para bancos de dados

Os fatores que determinam o número de tarefas de backup necessárias incluem o tamanho do banco de dados, o número de volumes usados, a taxa de alteração do banco de dados e seu Contrato de Nível de Serviço (SLA).

Para backups de banco de dados, o número de tarefas de backup que você escolhe normalmente depende do número de volumes nos quais você colocou seus bancos de dados. Por exemplo, se você colocar um grupo de bancos de dados pequenos em um volume e um banco de dados grande em outro volume, você poderá criar uma tarefa de backup para os bancos de dados pequenos e uma tarefa de backup para o banco de dados grande.

Convenções de nomenclatura de backup para plug-in para servidor SQL

Você pode usar a convenção de nomenclatura padrão do Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um registro de data e hora aos nomes de instantâneos que ajuda a identificar quando as cópias foram criadas.

O Snapshot usa a seguinte convenção de nomenclatura padrão:

```
resourcegroupname_hostname_timestamp
```

Você deve nomear seus grupos de recursos de backup logicamente, como no exemplo a seguir:

```
dts1_mach1x88_03-12-2015_23.17.26
```

Neste exemplo, os elementos de sintaxe têm os seguintes significados:

- *dts1* é o nome do grupo de recursos.
- *mach1x88* é o nome do host.
- *03-12-2015_23.17.26* é a data e o registro de data e hora.

Como alternativa, você pode especificar o formato do nome do Snapshot ao proteger recursos ou grupos de recursos selecionando **Usar formato de nome personalizado para cópia do Snapshot**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do registro de data e hora é adicionado ao nome do Snapshot.

Opções de retenção de backup para o Plug-in para SQL Server

Você pode escolher o número de dias pelos quais deseja manter cópias de backup ou especificar o número de cópias de backup que deseja manter, até um máximo ONTAP de 255 cópias. Por exemplo, sua organização pode exigir que você mantenha 10 dias de cópias de backup ou 130 cópias de backup.

Ao criar uma política, você pode especificar as opções de retenção para o tipo de backup e o tipo de agendamento.

Se você configurar a replicação do SnapMirror , a política de retenção será espelhada no volume de destino.

O SnapCenter exclui os backups retidos que têm rótulos de retenção que correspondem ao tipo de agendamento. Se o tipo de agendamento foi alterado para o recurso ou grupo de recursos, os backups com o rótulo de tipo de agendamento antigo ainda poderão permanecer no sistema.

Para retenção de cópias de backup a longo prazo, você deve usar o backup SnapVault .

Por quanto tempo manter backups de log de transações no sistema de armazenamento de origem

O plug-in SnapCenter para Microsoft SQL Server precisa de backups de log de transações para executar operações de restauração atualizadas, que restauram seu banco de dados para um intervalo entre dois backups completos.

Por exemplo, se o Plug-in para SQL Server fizesse um backup completo às 8h e outro backup completo às 17h, ele poderia usar o backup de log de transações mais recente para restaurar o banco de dados a qualquer momento entre 8h e 17h. Se os logs de transações não estiverem disponíveis, o Plug-in para SQL Server poderá executar apenas operações de restauração pontuais, que restauram um banco de dados ao momento em que o Plug-in para SQL Server concluiu um backup completo.

Normalmente, você precisa de operações de restauração atualizadas por apenas um ou dois dias. Por padrão, o SnapCenter retém no mínimo dois dias.

Vários bancos de dados no mesmo volume

Você pode colocar todos os bancos de dados no mesmo volume, porque a política de backup tem uma opção para definir o máximo de bancos de dados por backup (o valor padrão é 100).

Por exemplo, se você tiver 200 bancos de dados no mesmo volume, dois Snapshots serão criados com 100 bancos de dados em cada um dos dois Snapshots.

Verificação de cópia de backup usando o volume de armazenamento primário ou secundário para Plug-in para SQL Server

Você pode verificar cópias de backup no volume de armazenamento primário ou no volume de armazenamento secundário SnapMirror ou SnapVault . A verificação usando um volume de armazenamento secundário reduz a carga no volume de armazenamento primário.

Quando você verifica um backup que está no volume de armazenamento primário ou secundário, todos os Snapshots primários e secundários são marcados como verificados.

A licença SnapRestore é necessária para verificar cópias de backup no volume de armazenamento secundário SnapMirror e SnapVault .

Quando agendar trabalhos de verificação

Embora o SnapCenter possa verificar os backups imediatamente após criá-los, isso pode aumentar significativamente o tempo necessário para concluir o trabalho de backup e consome muitos recursos. Portanto, quase sempre é melhor agendar a verificação em uma tarefa separada para um momento posterior. Por exemplo, se você fizer backup de um banco de dados às 17h todos os dias, poderá agendar a verificação para ocorrer uma hora depois, às 18h.

Pelo mesmo motivo, geralmente não é necessário executar a verificação de backup toda vez que você faz um backup. Executar verificações em intervalos regulares, mas menos frequentes, geralmente é suficiente para garantir a integridade do backup. Uma única tarefa de verificação pode verificar vários backups ao mesmo tempo.

Estratégia de restauração para SQL Server

Origens e destinos para uma operação de restauração

Você pode restaurar um banco de dados do SQL Server a partir de uma cópia de backup

no armazenamento primário ou secundário. Você também pode restaurar o banco de dados para destinos diferentes além do seu local original, permitindo que você escolha o destino que atende às suas necessidades.

Fontes para uma operação de restauração

Você pode restaurar bancos de dados do armazenamento primário ou secundário.

Destinos para uma operação de restauração

Você pode restaurar bancos de dados para vários destinos:

Destino	Descrição
A localização original	Por padrão, o SnapCenter restaura o banco de dados no mesmo local na mesma instância do SQL Server.
Um local diferente	Você pode restaurar o banco de dados para um local diferente em qualquer instância do SQL Server no mesmo host.
Localização original ou diferente usando nomes de banco de dados diferentes	Você pode restaurar o banco de dados com um nome diferente para qualquer instância do SQL Server no mesmo host onde o backup foi criado.

Não há suporte para restauração em host alternativo entre servidores ESX para bancos de dados SQL em VMDKs (datastores NFS e VMFS).

Modelos de recuperação do SQL Server suportados pelo SnapCenter

Modelos de recuperação específicos são atribuídos a cada tipo de banco de dados por padrão. O administrador do banco de dados do SQL Server pode reatribuir cada banco de dados a um modelo de recuperação diferente.

O SnapCenter oferece suporte a três tipos de modelos de recuperação do SQL Server:

- Modelo de recuperação simples

  Ao usar o modelo de recuperação simples, você não pode fazer backup dos logs de transações.

- Modelo de recuperação total

  Ao usar o modelo de recuperação completa, você pode restaurar um banco de dados ao seu estado anterior a partir do ponto de falha.

- Modelo de recuperação de log em massa

  Ao usar o modelo de recuperação de log em massa, você deve reexecutar manualmente a operação de log em massa. Você deve executar a operação de registro em massa se o log de transações que contém o registro de confirmação da operação não tiver sido feito backup antes da restauração. Se a operação de registro em massa inserir 10 milhões de linhas em um banco de dados e o banco de dados falhar antes do backup do log de transações, o banco de dados restaurado não conterá as linhas que foram inseridas pela

operação de registro em massa.

Tipos de operações de restauração

Você pode usar o SnapCenter para executar diferentes tipos de operações de restauração em recursos do SQL Server.

- Restaurar atualizado
- Restaurar para um ponto anterior no tempo

Você pode restaurar até o minuto ou restaurar para um ponto anterior no tempo nas seguintes situações:

- Restaurar do armazenamento secundário SnapMirror ou SnapVault
- Restaurar para caminho alternativo (local)

O SnapCenter não oferece suporte ao SnapRestore baseado em volume.

Restaurar até o minuto

Em uma operação de restauração atualizada (selecionada por padrão), os bancos de dados são recuperados até o ponto de falha. O SnapCenter faz isso executando a seguinte sequência:

1. Faz backup do último log de transações ativo antes de restaurar o banco de dados.
2. Restaura os bancos de dados do backup completo do banco de dados selecionado.
3. Aplica todos os logs de transações que não foram confirmados nos bancos de dados (incluindo logs de transações dos backups desde o momento em que o backup foi criado até o momento mais recente).

   Os logs de transações são movidos e aplicados a quaisquer bancos de dados selecionados.

Uma operação de restauração atualizada requer um conjunto contíguo de logs de transações.

Como o SnapCenter não pode restaurar logs de transações do banco de dados SQL Server a partir de arquivos de backup de envio de logs (o envio de logs permite que você envie automaticamente backups de logs de transações de um banco de dados primário em uma instância do servidor primário para um ou mais bancos de dados secundários em instâncias separadas do servidor secundário), você não pode executar uma operação de restauração atualizada a partir dos backups de logs de transações. Por esse motivo, você deve usar o SnapCenter para fazer backup dos arquivos de log de transações do banco de dados SQL Server.

Se você não precisar manter a capacidade de restauração atualizada para todos os backups, poderá configurar a retenção de backup do log de transações do seu sistema por meio das políticas de backup.

Exemplo de uma operação de restauração atualizada

Suponha que você execute o backup do SQL Server todos os dias ao meio-dia e, na quarta-feira às 16h, você precise restaurar um backup. Por algum motivo, o backup de quarta-feira ao meio-dia falhou na verificação, então você decide restaurar o backup de terça-feira ao meio-dia. Depois disso, se o backup for restaurado, todos os logs de transações serão movidos para frente e aplicados aos bancos de dados restaurados, começando com aqueles que não foram confirmados quando você criou o backup de terça-feira e continuando até o último log de transações escrito na quarta-feira às 16h (se os logs de transações foram copiados).

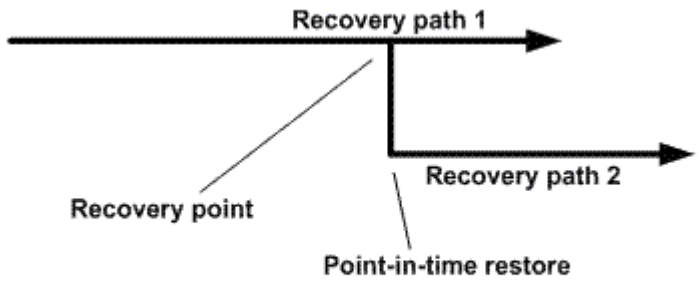
Restaurar para um ponto anterior no tempo

Em uma operação de restauração pontual, os bancos de dados são restaurados apenas para um momento específico do passado. Uma operação de restauração pontual ocorre nas seguintes situações de restauração:

- O banco de dados é restaurado para um determinado momento em um log de transações de backup.
- O banco de dados é restaurado e apenas um subconjunto de logs de transações de backup é aplicado a ele.

Restaurar um banco de dados para um ponto no tempo resulta em um novo caminho de recuperação.

A imagem a seguir ilustra os problemas quando uma operação de restauração de ponto no tempo é executada:



Na imagem, o caminho de recuperação 1 consiste em um backup completo seguido por vários backups de log de transações. Você restaura o banco de dados para um ponto no tempo. Novos backups de log de transações são criados após a operação de restauração de ponto no tempo, o que resulta no caminho de recuperação 2. Os novos backups do log de transações são criados sem criar um novo backup completo. Devido à corrupção de dados ou outros problemas, não é possível restaurar o banco de dados atual até que um novo backup completo seja criado. Além disso, não é possível aplicar os logs de transações criados no caminho de recuperação 2 ao backup completo pertencente ao caminho de recuperação 1.

Se você aplicar backups de log de transações, também poderá especificar uma data e hora específicas nas quais deseja interromper a aplicação das transações de backup. Para fazer isso, você especifica uma data e hora dentro do intervalo disponível e o SnapCenter remove todas as transações que não foram confirmadas antes desse momento. Você pode usar esse método para restaurar bancos de dados para um ponto no tempo anterior à ocorrência de uma corrupção ou para se recuperar de uma exclusão acidental de banco de dados ou tabela.

Exemplo de uma operação de restauração pontual

Suponha que você faça backups completos do banco de dados uma vez à meia-noite e um backup do log de transações a cada hora. O banco de dados falha às 9h45, mas você ainda faz backup dos logs de transações do banco de dados com falha. Você pode escolher entre estes cenários de restauração pontuais:

- Restaure o backup completo do banco de dados feito à meia-noite e aceite a perda das alterações feitas posteriormente no banco de dados. (Opção: Nenhuma)
- Restaurar o backup completo do banco de dados e aplicar todos os backups do log de transações até 9h45 (Opção: Logar até)

- Restaure o backup completo do banco de dados e aplique backups do log de transações, especificando o horário em que você deseja que as transações sejam restauradas do último conjunto de backups do log de transações. (Opção: Por horário específico)

Nesse caso, você calcularia a data e a hora em que um determinado erro foi relatado. Todas as transações que não foram confirmadas antes da data e hora especificadas serão removidas.

Definir uma estratégia de clonagem para o SQL Server

Definir uma estratégia de clonagem permite que você clone seu banco de dados com sucesso.

1. Revise as limitações relacionadas às operações de clonagem.
2. Decida o tipo de clone que você precisa.

Limitações das operações de clonagem

Você deve estar ciente das limitações das operações de clonagem antes de clonar os bancos de dados.

- Se você estiver usando qualquer versão do Oracle de 11.2.0.4 a 12.1.0.1, a operação de clonagem ficará travada quando você executar o comando *renamedg*. Você pode aplicar o patch 19544733 da Oracle para corrigir esse problema.
- A clonagem de bancos de dados de um LUN diretamente conectado a um host (por exemplo, usando o Microsoft iSCSI Initiator em um host Windows) para um VMDK ou um LUN RDM no mesmo host Windows ou em outro host Windows, ou vice-versa, não é suportada.
- O diretório raiz do ponto de montagem do volume não pode ser um diretório compartilhado.
- Se você mover um LUN que contém um clone para um novo volume, o clone não poderá ser excluído.

Tipos de operações de clonagem

Você pode usar o SnapCenter para clonar um backup de banco de dados do SQL Server ou um banco de dados de produção.

- Clonar de um backup de banco de dados

  O banco de dados clonado pode servir como base para o desenvolvimento de novos aplicativos e ajudar a isolar erros de aplicativo que ocorrem no ambiente de produção. O banco de dados clonado também pode ser usado para recuperação de erros leves de banco de dados.

- Ciclo de vida do clone

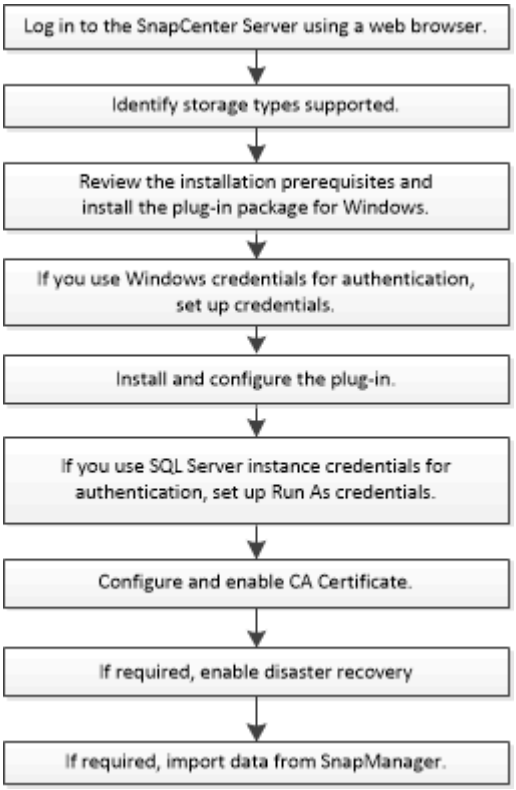
  Você pode usar o SnapCenter para agendar trabalhos de clonagem recorrentes que ocorrerão quando o banco de dados de produção não estiver ocupado.

Prepare-se para instalar o plug-in SnapCenter para Microsoft SQL Server

Fluxo de trabalho de instalação do plug-in SnapCenter para Microsoft SQL Server

Você deve instalar e configurar o SnapCenter Plug-in para Microsoft SQL Server se

quiser proteger bancos de dados do SQL Server.



Pré-requisitos para adicionar hosts e instalar o SnapCenter Plug-in para Microsoft SQL Server

Antes de adicionar um host e instalar os pacotes de plug-ins, você deve atender a todos os requisitos.

- Se você estiver usando iSCSI, o serviço iSCSI deverá estar em execução.
- Você deve ter um usuário com privilégios de administrador local com permissões de login local no host remoto.
- Se você gerenciar nós de cluster no SnapCenter, deverá ter um usuário com privilégios administrativos para todos os nós do cluster.
- Você deve ter um usuário com permissões de administrador de sistema no SQL Server.

  O plug-in SnapCenter para Microsoft SQL Server usa o Microsoft VDI Framework, que requer acesso de administrador de sistema.

  "Artigo de Suporte da Microsoft 2926557: As operações de backup e restauração do SQL Server VDI exigem privilégios de Sysadmin"

- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.
- Se o SnapManager para Microsoft SQL Server estiver instalado, você deverá ter interrompido ou desabilitado o serviço e os agendamentos.

  Se você planeja importar trabalhos de backup ou clonagem para o SnapCenter, não desinstale o

SnapManager para Microsoft SQL Server.

- O host deve ser resolvível para o nome de domínio totalmente qualificado (FQDN) do servidor.

  Se o arquivo hosts for modificado para torná-lo resolvível e se o nome abreviado e o FQDN forem especificados no arquivo hosts, crie uma entrada no arquivo hosts do SnapCenter no seguinte formato: <endereço_ip> <fqdn_do_host> <nome_do_host>

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows

Antes de instalar o pacote de plug-ins do SnapCenter para Windows, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas Operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	5 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.

Item	Requisitos
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK O Java 11 Oracle Java e OpenJDK são necessários apenas para SAP HANA, IBM Db2, PostgreSQL, MySQL, plug-ins compatíveis com NetApp e outros aplicativos personalizados que podem ser instalados no host Windows. Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."

Configurar credenciais para o pacote de plug-ins do SnapCenter para Windows

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter . Você deve criar credenciais para instalar plug-ins do SnapCenter e credenciais adicionais para executar operações de proteção de dados em bancos de dados ou sistemas de arquivos do Windows.

Antes de começar

- Você deve configurar as credenciais do Windows antes de instalar plug-ins.
- Você deve configurar as credenciais com privilégios de administrador, incluindo direitos de administrador no host remoto.
- Autenticação SQL em hosts Windows

  Você deve configurar credenciais SQL após instalar plug-ins.

  Se você estiver implantando o SnapCenter Plug-in para Microsoft SQL Server, deverá configurar as credenciais do SQL após instalar os plug-ins. Configure uma credencial para um usuário com permissões de administrador de sistema do SQL Server.

  O método de autenticação SQL autentica em uma instância do SQL Server. Isso significa que uma instância do SQL Server deve ser descoberta no SnapCenter. Portanto, antes de adicionar uma credencial SQL, você deve adicionar um host, instalar pacotes de plug-in e atualizar os recursos. Você precisa da autenticação do SQL Server para executar operações como agendamento ou descoberta de recursos.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.

2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.
4. Na página Credencial, especifique as informações necessárias para configurar as credenciais:

Para este campo…	Faça isso…
Nome da credencial	Digite um nome para a credencial.
Nome de usuário/Senha	Digite o nome de usuário e a senha que serão usados para autenticação. • Administrador de domínio Especifique o administrador de domínio do sistema no qual você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • Administrador local (somente para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é: `UserName` Não use aspas duplas (") ou acento grave (`) nas senhas. Você não deve usar os símbolos de menor que (<) e exclamação (!) juntos em senhas. Por exemplo, menor que <! 10, menor que 10 <!, acento grave `12.
Modo de autenticação	Selecione o modo de autenticação que você deseja usar. Se você selecionar o modo de autenticação SQL, também deverá especificar a instância do servidor SQL e o host onde a instância SQL está localizada.

5. Clique em **OK**.

Depois de concluir a configuração das credenciais, talvez você queira atribuir a manutenção de credenciais a

um usuário ou grupo de usuários na página Usuário e Acesso.

Configurar credenciais para um recurso individual do SQL Server

Você pode configurar credenciais para executar trabalhos de proteção de dados em recursos individuais do SQL Server para cada usuário. Embora você possa configurar as credenciais globalmente, talvez queira fazer isso apenas para um recurso específico.

Sobre esta tarefa

- Se estiver usando credenciais do Windows para autenticação, você deverá configurar suas credenciais antes de instalar plug-ins.

  No entanto, se você estiver usando uma instância do SQL Server para autenticação, deverá adicionar a credencial após instalar os plug-ins.

- Se você tiver habilitado a autenticação SQL ao configurar as credenciais, a instância ou o banco de dados descoberto será exibido com um ícone de cadeado vermelho.

  Se o ícone de cadeado aparecer, você deverá especificar as credenciais da instância ou do banco de dados para adicionar com sucesso a instância ou o banco de dados a um grupo de recursos.

- Você deve atribuir a credencial a um usuário de controle de acesso baseado em função (RBAC) sem acesso de administrador de sistema quando as seguintes condições forem atendidas:
  - A credencial é atribuída a uma instância SQL.
  - A instância ou host do SQL é atribuído a um usuário RBAC.

    O usuário deve ter privilégios de grupo de recursos e de backup.

Etapa 1: adicionar e configurar credenciais

1. No painel de navegação esquerdo, selecione **Configurações**.
2. Na página Configurações, selecione **Credencial**.
   a. Para adicionar uma nova credencial, selecione **Novo**.
   b. Na página Credencial, configure as credenciais:

Para este campo…	Faça isso…
Nome da credencial	Digite um nome para as credenciais.

Para este campo…	Faça isso…
Nome de usuário	Digite o nome de usuário usado para autenticação do SQL Server. • Administrador de domínio ou qualquer membro do grupo de administradores. Especifique o administrador de domínio ou qualquer membro do grupo de administradores no sistema no qual você está instalando o plug-in SnapCenter . Os formatos válidos para o campo **Nome de usuário** são: ◦ *NetBIOS\Nome do Usuário* ◦ *FQDN do domínio\Nome do usuário* • Administrador local (somente para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo **Nome de usuário** é: *Nome de usuário*
Senha	Digite a senha usada para autenticação.
Modo de autenticação	Selecione o modo de autenticação do SQL Server. Você também pode escolher a autenticação do Windows se o usuário do Windows tiver privilégios de administrador de sistema no servidor SQL.
Hospedar	Selecione o host.
Instância do SQL Server	Selecione a instância do SQL Server.

c. Selecione **OK** para adicionar a credencial.

Etapa 2: Configurar instâncias

1. No painel de navegação esquerdo, selecione **Recursos**.
2. Na página Recursos, selecione **Instância** na lista **Exibir**.
   a. Selecione image::../media/filter_icon.png[ícone de filtro] e, em seguida, selecione o nome do host para filtrar as instâncias.
   b. Selecione image::../media/filter_icon.png[ícone de filtro] para fechar o painel de filtro.
3. Na página Proteger instância, proteja a instância e, se necessário, selecione **Configurar credenciais**.

   Se o usuário conectado ao SnapCenter Server não tiver acesso ao SnapCenter Plugin para Microsoft SQL Server, ele precisará configurar as credenciais.

   A opção de credencial não se aplica a bancos de dados e grupos de disponibilidade.

4. Selecione **Atualizar recursos**.

Configurar o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite que você crie uma Conta de Serviço Gerenciada de grupo (gMSA) que fornece gerenciamento automatizado de senhas de contas de serviço a partir de uma conta de domínio gerenciada.

Antes de começar

- Você deve ter um controlador de domínio do Windows Server 2016 ou posterior.
- Você deve ter um host Windows Server 2016 ou posterior, que seja membro do domínio.

Passos

1. Crie uma chave raiz do KDS para gerar senhas exclusivas para cada objeto no seu gMSA.
2. Para cada domínio, execute o seguinte comando no controlador de domínio do Windows: Add-KDSRootKey -EffectiveImmediately
3. Crie e configure seu gMSA:
   a. Crie uma conta de grupo de usuários no seguinte formato:

```
 domainName\accountName$
.. Adicione objetos de computador ao grupo.
.. Use o grupo de usuários que você acabou de criar para criar o
gMSA.
```

   Por exemplo,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correr `Get-ADServiceAccount` comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Habilite o módulo do Active Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando no PowerShell:

```
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. Reinicie seu host.

b. Instale o gMSA no seu host executando o seguinte comando no prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua privilégios administrativos ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no SnapCenter Server.

   O SnapCenter Server instalará os plug-ins selecionados no host e o gMSA especificado será usado como a conta de logon de serviço durante a instalação do plug-in.

Instalar o plug-in SnapCenter para Microsoft SQL Server

Adicione hosts e instale o pacote de plug-ins SnapCenter para Windows

Você deve usar a página **Adicionar Host** do SnapCenter para adicionar hosts e instalar o pacote de plug-ins. Os plug-ins são instalados automaticamente nos hosts remotos.

Antes de começar

- Se o sistema operacional do host do SnapCenter Server for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deverá executar o seguinte:
  - Atualize para o Windows Server 2019 (versão do sistema operacional 17763.5936) ou posterior
  - Atualize para o Windows Server 2022 (versão do sistema operacional 20348.2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada, deverá desabilitar o UAC no host.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.

- Se estiver usando uma conta de serviço gerenciada em grupo (gMSA), você deverá configurar a gMSA com privilégios administrativos.

  "Configurar conta de serviço gerenciada de grupo no Windows Server 2016 ou posterior para SQL"

Sobre esta tarefa

Não é possível adicionar um SnapCenter Server como um host de plug-in a outro SnapCenter Server.

Você pode adicionar um host e instalar os pacotes de plug-in para um host individual ou para um cluster. Se você estiver instalando os plug-ins em um cluster ou no Windows Server Failover Clustering (WSFC), os plug-ins serão instalados em todos os nós do cluster.

Para obter informações sobre como gerenciar hosts, consulte"Gerenciar hosts" .

Passos

1. No painel de navegação esquerdo, selecione **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Selecione **Adicionar**.
4. Na página Hosts, faça o seguinte:

Para este campo…	Faça isso…
Tipo de host	Selecione Windows como o tipo de host. O SnapCenter Server adiciona o host e instala o plug-in para Windows, caso o plug-in ainda não esteja instalado no host. Se você selecionar a opção Microsoft SQL Server na página Plug-ins, o SnapCenter Server instalará o Plug-in para SQL Server.
Nome do host	Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O endereço IP é suportado para hosts de domínio não confiáveis somente se for resolvido para o FQDN. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o FQDN. Você pode inserir os endereços IP ou FQDN de um dos seguintes: • Host autônomo • WSFC Se você estiver adicionando um host usando o SnapCenter e o host fizer parte de um subdomínio, você deverá fornecer o FQDN.

Para este campo…	Faça isso…
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais. Você pode visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou. O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar Host.

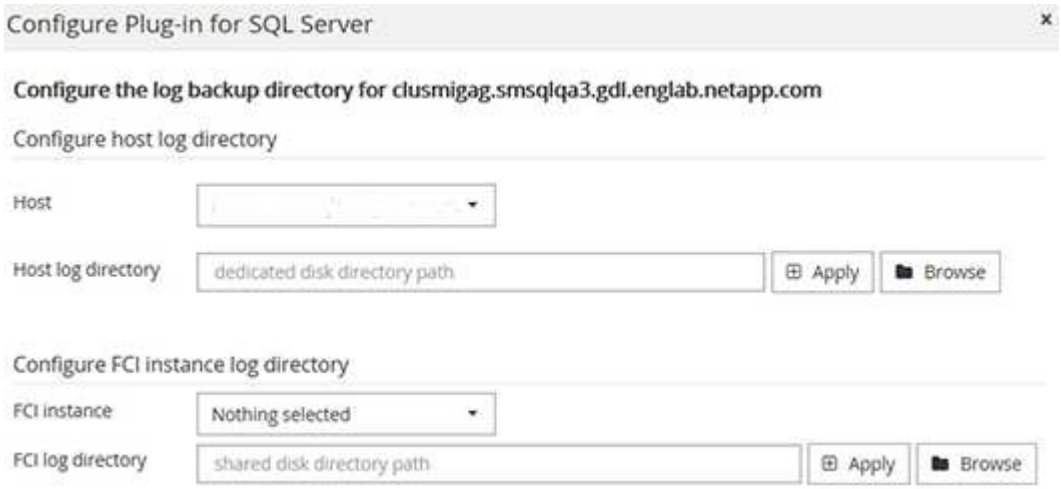
5. Na seção **Selecionar plug-ins para instalar**, selecione os plug-ins a serem instalados.
6. Selecione **Mais opções**.

Para este campo…	Faça isso…
Porta	Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.
Caminho de instalação	O caminho padrão é C:\Arquivos de Programas\ NetApp\ SnapCenter. Opcionalmente, você pode personalizar o caminho.
Adicionar todos os hosts no cluster	Marque esta caixa de seleção para adicionar todos os nós do cluster em um WSFC ou um Grupo de Disponibilidade SQL. Você deve adicionar todos os nós do cluster selecionando a caixa de seleção apropriada na GUI se quiser gerenciar e identificar vários Grupos de Disponibilidade de SQL disponíveis dentro de um cluster.
Ignorar verificações de pré-instalação	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.

Para este campo…	Faça isso…
Use a conta de serviço gerenciada em grupo (gMSA) para executar os serviços do plug-in	Marque esta caixa de seleção se desejar usar a Conta de Serviço Gerenciada em Grupo (gMSA) para executar os serviços do plug-in. Forneça o nome do gMSA no seguinte formato: domainName\accountName$. Se o host for adicionado com gMSA e se o gMSA tiver privilégios de login e administrador de sistema, o gMSA será usado para se conectar à instância do SQL.

7. Selecione **Enviar**.
8. Para o plug-in SQL, selecione o host para configurar o diretório de log.
   a. Selecione **Configurar diretório de log** e na página Configurar diretório de log do host, selecione **Procurar** e conclua as seguintes etapas:

      Somente LUNs (unidades) do NetApp são listados para seleção. O SnapCenter faz backup e replica o diretório de log do host como parte da operação de backup.



      i. Selecione a letra da unidade ou o ponto de montagem no host onde o log do host será armazenado.
      ii. Escolha um subdiretório, se necessário.
      iii. Selecione **Salvar**.
9. Selecione **Enviar**.

   Se você não tiver marcado a caixa de seleção **Ignorar pré-verificações**, o host será validado para verificar se atende aos requisitos para a instalação do plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão do .NET, a localização (para plug-ins do Windows) e a versão do Java (para plug-ins do Linux) são validados em relação aos requisitos mínimos. Se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas serão exibidas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config

localizado em C:\Arquivos de Programas\ NetApp\ SnapCenter WebApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.

> Em uma configuração de HA, se você estiver atualizando o arquivo web.config, deverá atualizar o arquivo em ambos os nós.

10. Monitore o progresso da instalação.

Instalar o plug-in SnapCenter para Microsoft SQL Server em vários hosts remotos usando cmdlets

Você pode instalar o SnapCenter Plug-in para Microsoft SQL Server em vários hosts simultaneamente usando o cmdlet Install-SmHostPackage do PowerShell.

Antes de começar

Você deve ter efetuado login no SnapCenter como um usuário de domínio com direitos de administrador local em cada host no qual deseja instalar o pacote de plug-in.

Passos

1. Inicie o PowerShell.
2. No host do SnapCenter Server, estabeleça uma sessão usando o cmdlet Open-SmConnection e insira suas credenciais.
3. Instale o SnapCenter Plug-in para Microsoft SQL Server em vários hosts remotos usando o cmdlet Install-SmHostPackage e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

   Você pode usar a opção -skipprecheck quando já tiver instalado os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

4. Insira suas credenciais para instalação remota.

Instale o plug-in SnapCenter para Microsoft SQL Server silenciosamente a partir da linha de comando

Você deve instalar o SnapCenter Plug-in para Microsoft SQL Server a partir da interface do usuário do SnapCenter . Entretanto, se por algum motivo você não puder, você pode executar o programa de instalação do Plug-in para SQL Server de forma autônoma no modo silencioso a partir da linha de comando do Windows.

Antes de começar

- Você deve excluir a versão anterior do SnapCenter Plug-in para Microsoft SQL Server antes de instalar.

  Para obter mais informações, consulte "Como instalar um plug-in SnapCenter manualmente e diretamente do host do plug-in" .

Passos

1. Valide se a pasta C:\temp existe no host do plug-in e se o usuário conectado tem acesso total a ela.
2. Baixe o plug-in para o software SQL Server em C:\ProgramData\ NetApp\ SnapCenter\Package Repository.

Este caminho pode ser acessado a partir do host onde o SnapCenter Server está instalado.

3. Copie o arquivo de instalação para o host no qual você deseja instalar o plug-in.
4. Em um prompt de comando do Windows no host local, navegue até o diretório onde você salvou os arquivos de instalação do plug-in.
5. Instale o plug-in para o software SQL Server:

```
"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
```

Substitua os valores do espaço reservado pelos seus dados

- Debug_Log_Path é o nome e o local do arquivo de log do instalador do pacote.
- Log_Path é o local dos logs de instalação dos componentes do plug-in (SCW, SCSQL e SMCore).
- Num é a porta na qual o SnapCenter se comunica com o SMCore
- Install_Directory_Path é o diretório de instalação do pacote de plug-in do host.
- domain\administrator é o plug-in SnapCenter para a conta de serviço web do Microsoft Windows.
- password é a senha para a conta de serviço web do SnapCenter Plug-in para Microsoft Windows.
  ```
  "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
  ```

> Todos os parâmetros passados durante a instalação do Plug-in para SQL Server diferenciam maiúsculas de minúsculas.

6. Monitore o agendador de tarefas do Windows, o arquivo de log de instalação principal C:\Installdebug.log e os arquivos de instalação adicionais em C:\Temp.
7. Monitore o diretório %temp% para verificar se os instaladores msiexe.exe estão instalando o software sem erros.

> A instalação do Plug-in para SQL Server registra o plug-in no host e não no SnapCenter Server. Você pode registrar o plug-in no SnapCenter Server adicionando o host usando a GUI do SnapCenter ou o cmdlet do PowerShell. Depois que o host é adicionado, o plug-in é descoberto automaticamente.

Monitore o status da instalação do Plug-in para SQL Server

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
   a. Clique em **Filtrar**.
   b. Opcional: especifique a data de início e término.
   c. No menu suspenso Tipo, selecione **Instalação de plug-in**.
   d. No menu suspenso Status, selecione o status da instalação.
   e. Clique em **Aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Configurar certificado CA

Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.

O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte "Como gerar um arquivo CSR de certificado CA" .

Se você possui o certificado CA para seu domínio (*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Importar chave privada	Selecione a opção **Sim**, importe a chave privada e clique em **Avançar**.
Formato de arquivo de importação	Não faça alterações; clique em **Avançar**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

> O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: *.pfx, *.p12 e *.p7b).

7. Repita a Etapa 5 para a pasta “Pessoal”.

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

Passos

1. Execute o seguinte na GUI:
   a. Clique duas vezes no certificado.
   b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.
   c. Percorra a lista de campos e clique em **Impressão digital**.
   d. Copie os caracteres hexadecimais da caixa.

e. Remova os espaços entre os números hexadecimais.

   Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
   a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copie a impressão digital.

Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Por exemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Vincule o certificado recém-instalado aos serviços de plug-in do host do Windows, executando os seguintes comandos:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

   Por exemplo:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *Get-SmCertificateSettings*.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- *  * indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- *  * indica que o certificado CA foi validado com sucesso.
- *  * indica que o certificado CA não pôde ser validado.
- *  * indica que as informações de conexão não puderam ser recuperadas.

Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Configurar recuperação de desastres

Recuperação de desastres do plug-in SnapCenter para SQL Server

Quando o plug-in SnapCenter para SQL Server estiver inativo, use as etapas a seguir para alternar para um host SQL diferente e recuperar os dados.

Antes de começar

- O host secundário deve ter o mesmo sistema operacional, aplicativo e nome de host que o host primário.
- Envie o plug-in SnapCenter para SQL Server para um host alternativo usando a página **Adicionar host** ou **Modificar host**. Ver "Gerenciar hosts" para maiores informações.

Passos

1. Selecione o host na página **Hosts** para modificar e instalar o SnapCenter Plug-in para SQL Server.

2. (Opcional) Substitua os arquivos de configuração do SnapCenter Plug-in para SQL Server do backup de recuperação de desastres (DR) para a nova máquina.
3. Importe agendamentos do Windows e do SQL da pasta SnapCenter Plug-in para SQL Server do backup de DR.

Informações relacionadas

Veja o"APIs de recuperação de desastres" vídeo.

Recuperação de desastres de armazenamento (DR) para o plug-in SnapCenter para SQL Server

Você pode recuperar o plug-in SnapCenter para armazenamento do SQL Server habilitando o Modo DR para Armazenamento na página Configurações Globais.

Antes de começar

- Certifique-se de que os plug-ins estejam no modo de manutenção.
- Rompa o relacionamento SnapMirror/ SnapVault ."Quebrando relacionamentos do SnapMirror"
- Anexe o LUN do secundário à máquina host com a mesma letra de unidade.
- Certifique-se de que todos os discos estejam conectados usando as mesmas letras de unidade que eram usadas antes do DR.
- Reinicie o serviço do servidor MSSQL.
- Certifique-se de que os recursos SQL estejam online novamente.

Sobre esta tarefa

A recuperação de desastres (DR) não é suportada em configurações VMDK e RDM.

Passos

1. Na página Configurações, navegue até **Configurações** > **Configurações globais** > **Recuperação de desastres**.
2. Selecione **Ativar recuperação de desastres**.
3. Clique em **Aplicar**.
4. Verifique se o trabalho de DR está habilitado ou não clicando em **Monitor** > **Trabalhos**.

Depois que você terminar

- Se novos bancos de dados forem criados após o failover, eles estarão no modo não DR.

  Os novos bancos de dados continuarão operando como antes do failover.

- Os novos backups criados no modo DR serão listados em SnapMirror ou SnapVault (secundário) na página Topologia.

  Um ícone "i" é exibido ao lado dos novos backups para indicar que esses backups foram criados durante o modo DR.

- Você pode excluir os backups do SnapCenter Plug-in para SQL Server que foram criados durante o failover usando a interface do usuário ou o seguinte cmdlet: `Remove-SmBackup`
- Após o failover, se você quiser que alguns recursos estejam no modo não DR, use o seguinte cmdlet: `Remove-SmResourceDRMode`

Para mais informações consulte o "Guia de referência do cmdlet do software SnapCenter" .

- O SnapCenter Server gerenciará os recursos de armazenamento individuais (bancos de dados SQL) que estão no modo DR ou não DR, mas não o grupo de recursos com recursos de armazenamento que estão no modo DR ou não DR.

Failback do plug-in SnapCenter para armazenamento secundário do SQL Server para armazenamento primário

Depois que o plug-in SnapCenter para armazenamento primário do SQL Server estiver online novamente, você deverá fazer failback para o armazenamento primário.

Antes de começar

- Coloque o SnapCenter Plug-in para SQL Server no modo **Manutenção** na página Hosts Gerenciados.
- Desconecte o armazenamento secundário do host e conecte-o do armazenamento primário.
- Para fazer failback para o armazenamento primário, certifique-se de que a direção do relacionamento permaneça a mesma de antes do failover, executando a operação de ressincronização reversa.

  Para manter as funções de armazenamento primário e secundário após a operação de ressincronização reversa, execute a operação de ressincronização reversa mais uma vez.

  Para mais informações, consulte"Ressincronização reversa de relacionamentos de espelho"

- Reinicie o serviço do servidor MSSQL.
- Certifique-se de que os recursos SQL estejam online novamente.

> Durante o failover ou failback do plug-in, o status geral do plug-in não é atualizado imediatamente. O status geral do host e do plug-in é atualizado durante a operação de atualização do host subsequente.

Passos

1. Na página Configurações, navegue até **Configurações** > **Configurações globais** > **Recuperação de desastres**.
2. Desmarque **Ativar recuperação de desastres**.
3. Clique em **Aplicar**.
4. Verifique se o trabalho de DR está habilitado ou não clicando em **Monitor** > **Trabalhos**.

Depois que você terminar

Você pode excluir os backups do SnapCenter Plug-in para SQL Server que foram criados durante o failover usando a interface do usuário ou o seguinte cmdlet: `Remove-SmDRFailoverBackups`

Instalar o SnapCenter Plug-in for VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs), ou se você quiser proteger VMs e armazenamentos de dados, será necessário implantar o SnapCenter Plug-in for VMware vSphere .

Para obter informações sobre como implantar, consulte "Visão geral da implantação" .

Implantar certificado CA

Para configurar o Certificado CA com o SnapCenter Plug-in for VMware vSphere, consulte "Criar ou importar certificado SSL" .

Configurar o arquivo CRL

O SnapCenter Plug-in for VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL do SnapCenter Plug-in for VMware vSphere é */opt/netapp/config/crl*.

Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Prepare-se para a proteção de dados

Pré-requisitos para usar o SnapCenter Plug-in para Microsoft SQL Server

Antes de começar a usar o Plug-in para SQL Server, o administrador do SnapCenter deve instalar e configurar o SnapCenter Server e executar tarefas de pré-requisito.

- Instalar e configurar o SnapCenter Server.
- Efetue login no SnapCenter.
- Configure o ambiente SnapCenter adicionando ou atribuindo conexões do sistema de armazenamento e criando credenciais.

> ⓘ O SnapCenter não oferece suporte a várias SVMs com o mesmo nome em clusters diferentes. Cada SVM suportado pelo SnapCenter deve ter um nome exclusivo.

- Adicione hosts, instale os plug-ins, descubra (atualize) os recursos e configure os plug-ins.
- Mova um banco de dados existente do Microsoft SQL Server de um disco local para um LUN do NetApp ou vice-versa executando Invoke-SmConfigureResources.

  Para obter informações sobre como executar o cmdlet, consulte o "Guia de referência do cmdlet do software SnapCenter"

- Se você estiver usando o SnapCenter Server para proteger bancos de dados SQL que residem em LUNs ou VMDKs do VMware RDM, será necessário implantar o SnapCenter Plug-in for VMware vSphere e registrar o plug-in no SnapCenter. A documentação do SnapCenter Plug-in for VMware vSphere tem mais informações.

  "Documentação do SnapCenter Plug-in for VMware vSphere"

- Execute o provisionamento de armazenamento do lado do host usando o plug-in SnapCenter para Microsoft Windows.
- Configure relacionamentos SnapMirror e SnapVault , se desejar replicação de backup.

Para obter detalhes, consulte as informações de instalação do SnapCenter .

Para usuários do SnapCenter 4.1.1, a documentação do SnapCenter Plug-in for VMware vSphere 4.1.1 contém informações sobre como proteger bancos de dados e sistemas de arquivos virtualizados. Para usuários do SnapCenter 4.2.x, a documentação do NetApp Data Broker 1.0 e 1.0.1 contém informações sobre

como proteger bancos de dados virtualizados e sistemas de arquivos usando o SnapCenter Plug-in for VMware vSphere fornecido pelo dispositivo virtual NetApp Data Broker baseado em Linux (formato Open Virtual Appliance). Para usuários do SnapCenter 4.3.x, a documentação do SnapCenter Plug-in for VMware vSphere 4.3 contém informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o dispositivo virtual SnapCenter Plug-in for VMware vSphere baseado em Linux (formato Open Virtual Appliance).

"Documentação do SnapCenter Plug-in for VMware vSphere"

Como recursos, grupos de recursos e políticas são usados para proteger o SQL Server

Antes de usar o SnapCenter, é útil entender os conceitos básicos relacionados às operações de backup, clonagem e restauração que você deseja executar. Você interage com recursos, grupos de recursos e políticas para diferentes operações.

- Os recursos geralmente são bancos de dados, instâncias de banco de dados ou grupos de disponibilidade do Microsoft SQL Server que você faz backup ou clona com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host ou cluster.

  Ao executar uma operação em um grupo de recursos, você executa essa operação nos recursos definidos no grupo de recursos de acordo com o cronograma especificado para o grupo de recursos.

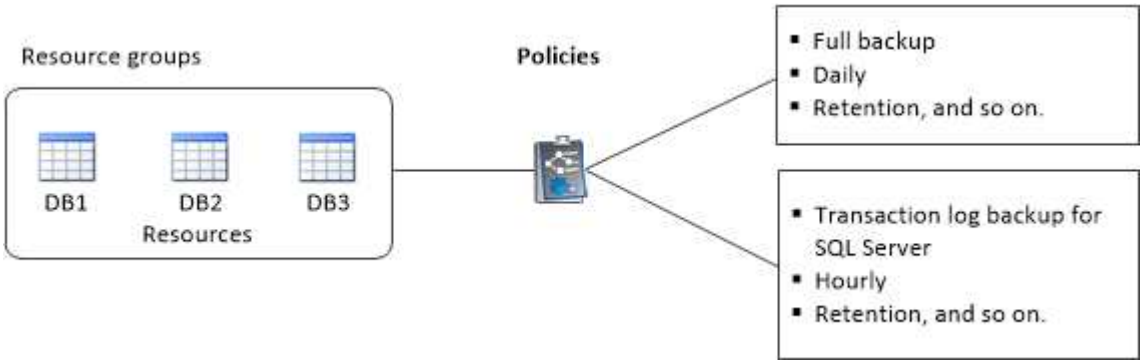
  Você pode fazer backup sob demanda de um único recurso ou de um grupo de recursos. Você também pode executar backups agendados para recursos individuais e grupos de recursos.

- As políticas especificam a frequência de backup, retenção de cópias, replicação, scripts e outras características das operações de proteção de dados.

  Ao criar um grupo de recursos, você seleciona uma ou mais políticas para esse grupo. Você também pode selecionar uma política ao executar um backup sob demanda para um único recurso.

Pense em um grupo de recursos como definidor de *o que* você quer proteger e quando quer proteger em termos de dia e hora. Pense em uma política como a definição de *como* você quer protegê-la. Se você estiver fazendo backup de todos os bancos de dados ou de todos os sistemas de arquivos de um host, por exemplo, poderá criar um grupo de recursos que inclua todos os bancos de dados ou todos os sistemas de arquivos no host. Você pode então anexar duas políticas ao grupo de recursos: uma política diária e uma política horária. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diariamente e outra programação que executa backups de log a cada hora.

A imagem a seguir ilustra o relacionamento entre recursos, grupos de recursos e políticas para bancos de dados:



Fazer backup do banco de dados, instância ou grupo de disponibilidade do SQL Server

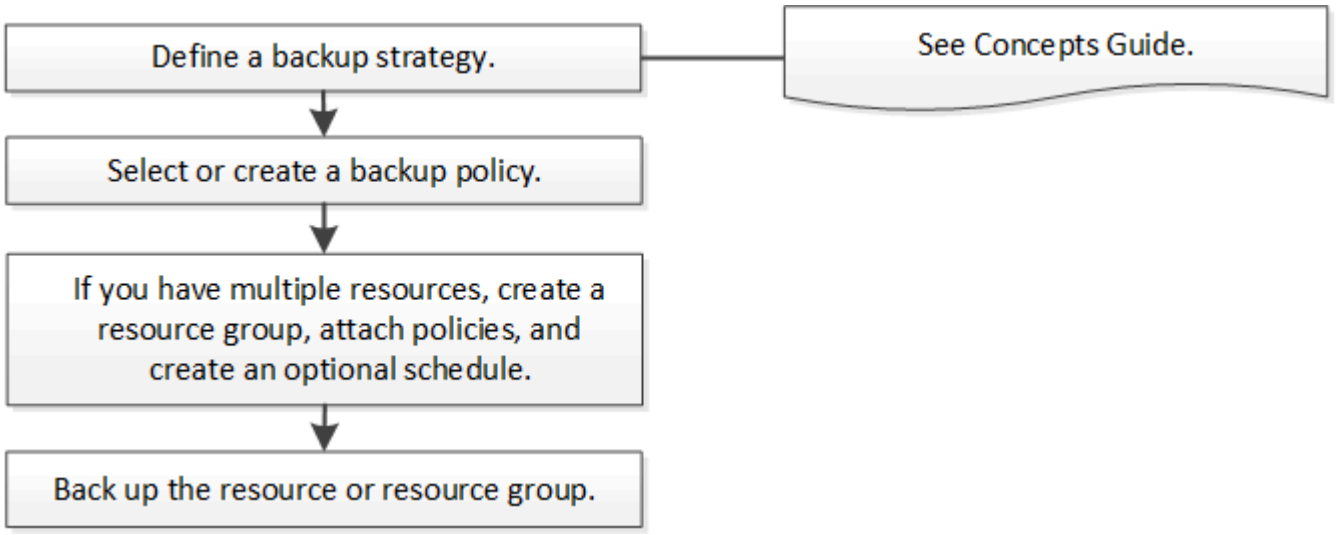
Fluxo de trabalho de backup

Ao instalar o SnapCenter Plug-in para Microsoft SQL Server em seu ambiente, você pode usar o SnapCenter para fazer backup dos recursos do SQL Server.

Você pode agendar vários backups para serem executados em todos os servidores simultaneamente.

As operações de backup e restauração não podem ser executadas simultaneamente no mesmo recurso.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar as operações de backup:



As opções Fazer backup agora, Restaurar, Gerenciar backups e Clonar na página Recursos serão desabilitadas se você selecionar um LUN que não seja da NetApp , um banco de dados corrompido ou um banco de dados que esteja sendo restaurado.

Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração, recuperação, verificação e clonagem. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet do SnapCenter ou consulte o "Guia de referência do cmdlet do software SnapCenter"

Como o SnapCenter faz backup de bancos de dados

O SnapCenter usa a tecnologia Snapshot para fazer backup dos bancos de dados do SQL Server que residem em LUNs ou VMDKs. O SnapCenter cria o backup criando instantâneos dos bancos de dados.

Quando você seleciona um banco de dados para um backup completo na página Recursos, o SnapCenter seleciona automaticamente todos os outros bancos de dados que residem no mesmo volume de armazenamento. Se o LUN ou VMDK armazenar apenas um único banco de dados, você poderá limpar ou selecionar novamente o banco de dados individualmente. Se o LUN ou VMDK abrigar vários bancos de dados, você deverá limpar ou selecionar novamente os bancos de dados como um grupo.

Todos os bancos de dados que residem em um único volume são copiados simultaneamente usando Snapshots. Se o número máximo de bancos de dados de backup simultâneos for 35 e se mais de 35 bancos

de dados residirem em um volume de armazenamento, o número total de Snapshots criados será igual ao número de bancos de dados dividido por 35.

Você pode configurar o número máximo de bancos de dados para cada Snapshot na política de backup.

Quando o SnapCenter cria um Snapshot, todo o volume do sistema de armazenamento é capturado no Snapshot. No entanto, o backup é válido somente para o servidor host SQL para o qual o backup foi criado.

Se dados de outros servidores host SQL residirem no mesmo volume, esses dados não poderão ser restaurados do Snapshot.

Encontre mais informações

"As operações de agrupamento ou de desativação de recursos falham"

Determinar se há recursos disponíveis para backup

Os recursos são bancos de dados, instâncias de aplicativos, grupos de disponibilidade e componentes semelhantes que são mantidos pelos plug-ins que você instalou. Você pode adicionar esses recursos a grupos de recursos para poder executar tarefas de proteção de dados, mas primeiro você deve identificar quais recursos estão disponíveis. Determinar os recursos disponíveis também verifica se a instalação do plug-in foi concluída com sucesso.

Antes de começar

- Você já deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts, criar conexões do sistema de armazenamento e adicionar credenciais.
- Para descobrir os bancos de dados do Microsoft SQL, uma das seguintes condições deve ser atendida.
  - O usuário usado para adicionar o host do plug-in ao SnapCenter Server deve ter as permissões necessárias (sysadmin) no Microsoft SQL Server.
  - Se a condição acima não for atendida, no SnapCenter Server você deve configurar o usuário que tem as permissões necessárias (sysadmin) no Microsoft SQL Server. O usuário deve ser configurado no nível da instância do Microsoft SQL Server e pode ser um usuário do SQL ou do Windows.
- Para descobrir os bancos de dados Microsoft SQL em um cluster do Windows, você deve desbloquear a porta TCP/IP da instância do cluster de failover (FCI).
- Se os bancos de dados residirem em LUNs ou VMDKs do VMware RDM, você deverá implantar o SnapCenter Plug-in for VMware vSphere e registrar o plug-in no SnapCenter.

  Para mais informações, consulte "Implantar o SnapCenter Plug-in for VMware vSphere"
- Se o host for adicionado com gMSA e se o gMSA tiver privilégios de login e administrador do sistema, o gMSA será usado para se conectar à instância do SQL.

Sobre esta tarefa

Não é possível fazer backup de bancos de dados quando a opção **Status geral** na página Detalhes estiver definida como Não disponível para backup. A opção **Status geral** é definida como Não disponível para backup quando qualquer uma das seguintes condições for verdadeira:

- Os bancos de dados não estão em um LUN do NetApp .

- Os bancos de dados não estão em estado normal.

  Os bancos de dados não estão em estado normal quando estão offline, restaurando, com recuperação pendente, suspeitos e assim por diante.

- Os bancos de dados não têm privilégios suficientes.

  Por exemplo, se um usuário tiver apenas acesso de visualização ao banco de dados, os arquivos e propriedades do banco de dados não poderão ser identificados e, portanto, não poderão ser copiados.

O SnapCenter pode fazer backup somente do banco de dados primário se você tiver uma configuração de grupo de disponibilidade no SQL Server Standard Edition.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados**, ou **Instância**, ou **Grupo de disponibilidade**, na lista suspensa **Exibir**.

   Clique e selecione o nome do host e a instância do SQL Server para filtrar os recursos. Você pode então clicar para fechar o painel de filtro.

3. Clique em **Atualizar recursos**.

   Os recursos recém-adicionados, renomeados ou excluídos são atualizados para o inventário do SnapCenter Server.

   Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

   Os recursos são exibidos junto com informações como tipo de recurso, nome do host ou cluster, grupos de recursos associados, tipo de backup, políticas e status geral.

   - Se o banco de dados estiver em um armazenamento não NetApp , `Not available for backup` é exibido na coluna **Status geral**.

     Não é possível executar operações de proteção de dados em um banco de dados que esteja em um armazenamento que não seja da NetApp .

   - Se o banco de dados estiver em um armazenamento NetApp e não estiver protegido, `Not protected` é exibido na coluna **Status geral**.
   - Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, a interface do usuário exibirá `Backup not run` mensagem na coluna **Status geral**.
   - Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido e se o backup for acionado para o banco de dados, a interface do usuário exibirá `Backup succeeded` mensagem na coluna **Status geral**.

   Se você tiver habilitado uma autenticação SQL ao configurar as credenciais, a instância ou banco de dados descoberto será mostrado com um ícone de cadeado vermelho. Se o ícone de cadeado aparecer, você deverá especificar as credenciais da instância ou do banco de dados para adicionar com sucesso a instância ou o banco de dados a um grupo de recursos.

1. Depois que o administrador do SnapCenter atribui os recursos a um usuário do RBAC, o usuário do RBAC deve efetuar login e clicar em **Atualizar recursos** para ver o **Status geral** mais recente dos recursos.

Migrar recursos para o sistema de armazenamento NetApp

Depois de provisionar seu sistema de armazenamento NetApp usando o SnapCenter Plug-in para Microsoft Windows, você pode migrar seus recursos para o sistema de armazenamento NetApp ou de um NetApp LUN para outro NetApp LUN usando a interface gráfica do usuário (GUI) do SnapCenter ou os cmdlets do PowerShell.

Antes de começar

- Você deve ter adicionado sistemas de armazenamento ao SnapCenter Server.
- Você deve ter atualizado (descoberto) os recursos do SQL Server.

A maioria dos campos nessas páginas do assistente são autoexplicativos. As informações a seguir descrevem alguns dos campos para os quais você pode precisar de orientação.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Instância** na lista suspensa **Exibir**.
3. Selecione o banco de dados ou a instância na lista e clique em **Migrar**.
4. Na página Recursos, execute as seguintes ações:

Para este campo…	Faça isso…
Nome do banco de dados (opcional)	Se você selecionou uma instância para migração, deverá selecionar os bancos de dados dessa instância na lista suspensa **Bancos de dados**.
Escolha Destinos	Selecione o local de destino para os dados e arquivos de log. Os arquivos de dados e log são movidos para as pastas Dados e Log, respectivamente, na unidade NetApp selecionada. Se alguma pasta na estrutura de pastas não estiver presente, uma pasta será criada e o recurso será migrado.
Mostrar detalhes do arquivo de banco de dados (opcional)	Selecione esta opção quando quiser migrar vários arquivos de um único banco de dados. Esta opção não é exibida quando você seleciona o recurso **Instância**.

Para este campo…	Faça isso…
Opções	Selecione **Excluir cópia do banco de dados migrado no local original** para excluir uma cópia do banco de dados da origem. Opcional: **EXECUTAR ATUALIZAÇÃO DE ESTATÍSTICAS nas tabelas antes de desanexar o banco de dados**.

5. Na página Verificar, execute as seguintes ações:

Para este campo…	Faça isso…
Opções de verificação de consistência do banco de dados	Selecione **Executar antes** para verificar a integridade do banco de dados antes da migração. Selecione **Executar após** para verificar a integridade do banco de dados após a migração.
Opções DBCC CHECKDB	• Selecione a opção **PHYSICAL_ONLY** para limitar a verificação de integridade à estrutura física do banco de dados e detectar páginas quebradas, falhas de soma de verificação e falhas comuns de hardware que afetam o banco de dados. • Selecione a opção **NO_INFOMSGS** para suprimir todas as mensagens informativas. • Selecione a opção **ALL_ERRORMSGS** para exibir todos os erros relatados por objeto. • Selecione a opção **NOINDEX** se não quiser verificar índices não agrupados. O banco de dados SQL Server usa o Microsoft SQL Server Database Consistency Checker (DBCC) para verificar a integridade lógica e física dos objetos no banco de dados. Talvez você queira selecionar esta opção para diminuir o tempo de execução. • Selecione a opção **TABLOCK** para limitar as verificações e obter bloqueios em vez de usar um instantâneo interno do banco de dados.

6. Revise o resumo e clique em **Concluir**.

Crie políticas de backup para bancos de dados SQL Server

Você pode criar uma política de backup para o recurso ou grupo de recursos antes de

usar o SnapCenter para fazer backup de recursos do SQL Server ou pode criar uma política de backup no momento em que cria um grupo de recursos ou faz backup de um único recurso.

Antes de começar

- Você deve ter definido sua estratégia de proteção de dados.
- Você deve estar preparado para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, identificar recursos e criar conexões de sistema de armazenamento.
- Você deve ter configurado o diretório de log do host para backup de log.
- Você deve ter atualizado (descoberto) os recursos do SQL Server.
- Se você estiver replicando Snapshots para um espelho ou cofre, o administrador do SnapCenter deverá ter atribuído as máquinas virtuais de armazenamento (SVMs) para os volumes de origem e de destino a você.

  Para obter informações sobre como os administradores atribuem recursos aos usuários, consulte as informações de instalação do SnapCenter .

- Se você quiser executar os scripts do PowerShell em prescripts e postscripts, defina o valor do parâmetro usePowershellProcessforScripts como true no arquivo web.config.

  O valor padrão é falso.

- Revise os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror . Para obter informações, consulte "Limites de objetos para sincronização ativa do SnapMirror" .

Sobre esta tarefa

- Uma política de backup é um conjunto de regras que rege como você gerencia e mantém backups e com que frequência o recurso ou grupo de recursos é feito backup. Além disso, você pode especificar configurações de replicação e script. Especificar opções em uma política economiza tempo quando você deseja reutilizar a política para outro grupo de recursos.

  O SCRIPTS_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCoreServiceHost.exe.Config do host do plug-in.

  Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável que você use o caminho padrão por segurança.

  O valor da chave pode ser exibido no swagger por meio da API: API /4.7/configsettings

  Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

- SnapLock

  - Se a opção 'Manter as cópias de backup por um número específico de dias' for selecionada, o período de retenção do SnapLock deverá ser menor ou igual aos dias de retenção mencionados.

    Especificar um período de bloqueio de Snapshot impede a exclusão dos Snapshots até que o período de retenção expire. Isso pode levar à retenção de um número maior de Snapshots do que a contagem especificada na política.

  Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de

armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Etapa 1: Criar nome da política

1. No painel de navegação esquerdo, selecione **Configurações**.
2. Na página Configurações, selecione **Políticas**.
3. Selecione **Novo**.
4. Na página **Nome**, insira o nome e os detalhes da política.

Etapa 2: Configurar opções de política

1. Na página Tipo de política, execute as seguintes etapas:
   a. Selecione seu tipo de armazenamento.
   b. Selecione o escopo da sua política.

Backup completo e backup de log

Faça backup dos arquivos de banco de dados e dos logs de transações e trunque os logs de transações.

i. Selecione **Backup completo e Backup de log**.

ii. Insira o número máximo de bancos de dados que devem ser copiados para cada Snapshot.

> Você deve aumentar esse valor se quiser executar várias operações de backup simultaneamente.

Backup completo

Faça backup dos arquivos do banco de dados.

i. Selecione **Backup completo**.

ii. Insira o número máximo de bancos de dados que devem ser copiados para cada Snapshot. O valor padrão é 100

> Você deve aumentar esse valor se quiser executar várias operações de backup simultaneamente.

Backup de log

i. Faça backup dos logs de transações.

ii. Selecione **Backup de log**.

Backup somente cópia

i. Se você estiver fazendo backup de seus recursos usando outro aplicativo de backup, selecione **Copiar somente backup**.

Manter os logs de transações intactos permite que qualquer aplicativo de backup restaure os bancos de dados. Normalmente, você não deve usar a opção somente cópia em nenhuma outra circunstância.

> O Microsoft SQL não oferece suporte à opção **Somente cópia de backup** juntamente com as opções **Backup completo e Backup de log** para armazenamento secundário.

Etapa 3: Configurar as configurações do Grupo de Disponibilidade

1. Na seção Configurações do grupo de disponibilidade, execute as seguintes ações:

   a. Faça backup somente na réplica de backup preferencial.

      Selecione esta opção para fazer backup somente na réplica de backup preferida. A réplica de backup preferencial é decidida pelas preferências de backup configuradas para o AG no SQL Server.

   b. Selecione réplicas para backup.

      Escolha a réplica do AG primário ou a réplica do AG secundário para o backup.

c. Selecione a prioridade de backup (prioridade mínima e máxima de backup)

   Especifique um número mínimo de prioridade de backup e um número máximo de prioridade de backup que decidam a réplica do AG para backup. Por exemplo, você pode ter uma prioridade mínima de 10 e uma prioridade máxima de 50. Nesse caso, todas as réplicas do AG com prioridade maior que 10 e menor que 50 são consideradas para backup.

   Por padrão, a prioridade mínima é 1 e a máxima é 100.

> Em configurações de cluster, os backups são retidos em cada nó do cluster de acordo com as configurações de retenção definidas na política. Se o nó proprietário do AG for alterado, os backups serão feitos de acordo com as configurações de retenção e os backups do nó proprietário anterior serão mantidos. A retenção para AG é aplicável somente no nível do nó.

Etapa 4: Configurar as configurações de instantâneo e replicação

1. Na página Snapshot e Replicação, execute as seguintes etapas:

   a. Especifique o tipo de programação selecionando **Sob demanda**, **Por hora**, **Diário**, **Semanal** ou **Mensal**.

      Você só pode selecionar um tipo de agendamento para uma política.

> Você pode especificar o agendamento (data de início, data de término e frequência) para a operação de backup ao criar um grupo de recursos. Isso permite que você crie grupos de recursos que compartilham a mesma política e frequência de backup, mas permite que você atribua agendamentos de backup diferentes a cada política.

> Se você agendou para 2h00, a programação não será acionada durante o horário de verão (DST).

Etapa 5: Configurar as configurações de retenção mais recentes

1. Na seção Configurações de retenção atualizadas, dependendo do tipo de backup selecionado na página de tipo de backup, execute uma ou mais das seguintes ações:

Número específico de cópias

Mantenha apenas um número específico de Snapshots.

1. Selecione a opção **Manter backups de log aplicáveis aos últimos <número> dias** e especifique o número de dias a serem retidos. Se você estiver próximo desse limite, talvez seja melhor excluir cópias mais antigas.

Número específico de dias

Mantenha as cópias de segurança por um número específico de dias.

1. Selecione a opção **Manter backups de log aplicáveis aos últimos <número> dias de backups completos** e especifique o número de dias para manter as cópias de backup de log.

Etapa 6: Configurar as definições do Snapshot

1. Para as configurações de retenção de backup completo, execute as seguintes ações:

   a. Especifique o número total de instantâneos a serem mantidos

      i. Para especificar o número de instantâneos a serem mantidos, selecione **Cópias a serem mantidas**.

      ii. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos, com as cópias mais antigas sendo excluídas primeiro.

      Por padrão, o valor da contagem de retenção é definido como 2. Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro instantâneo será o instantâneo de referência para o relacionamento SnapVault até que um instantâneo mais recente seja replicado para o destino.

   O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida como um valor maior do que o suportado pela versão subjacente do NetApp ONTAP .

2. Período de tempo para manter instantâneos

   a. Se você quiser especificar o número de dias pelos quais deseja manter os instantâneos antes de excluí-los, selecione **Manter cópias por**.

3. Selecione **Período de bloqueio de cópia de instantâneo** e especifique a duração em dias, meses ou anos.

   O período de retenção do Snaplock deve ser inferior a 100 anos.

4. Selecione um rótulo de política.

   Você pode atribuir rótulos SnapMirror a snapshots primários para replicação remota, permitindo que os snapshots primários descarreguem a operação de replicação de snapshots do SnapCenter para sistemas secundários ONTAP . Isso pode ser feito sem habilitar a opção SnapMirror ou SnapVault na página de política.

Etapa 7: Configurar opções de replicação secundária

1. Na seção Selecionar opções de replicação secundária, selecione uma ou ambas as seguintes opções de replicação secundária:

Atualizar SnapMirror

Atualize o SnapMirror após criar uma cópia local do Snapshot.

1. Selecione esta opção para criar cópias espelhadas de conjuntos de backup em outro volume (SnapMirror).

   Esta opção deve ser habilitada para sincronização ativa do SnapMirror .

   Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP.

   Ver "Exibir backups e clones do SQL Server na página Topologia" .

Atualizar SnapVault

Atualize o SnapVault após criar uma cópia do Snapshot.

1. Selecione esta opção para executar a replicação de backup de disco para disco.

   Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP.

   Quando o SnapLock é configurado somente no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página Topologia atualiza o período de bloqueio no secundário recuperado do ONTAP.

   Para mais informações sobre o SnapLock Vault, consulte "Enviar cópias do Snapshot para o WORM em um destino de cofre"

   Ver "Exibir backups e clones do SQL Server na página Topologia" .

Contagem de novas tentativas de erro

1. Insira o número de tentativas de replicação que devem ocorrer antes que o processo seja interrompido.

Etapa 8: Configurar as definições do script

1. Na página Script, insira o caminho e os argumentos do prescript ou postscript que devem ser executados antes ou depois da operação de backup, respectivamente.

   Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas e enviar logs.

   O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_PATH.

   Você deve configurar a política de retenção do SnapMirror no ONTAP para que o armazenamento secundário não atinja o limite máximo de Snapshots.

Etapa 9: Configurar as configurações de verificação

Na página Verificação, execute as seguintes etapas:

1. Na seção Executar verificação para os seguintes agendamentos de backup, selecione a frequência do agendamento.
2. Na seção Opções de verificação de consistência do banco de dados, execute as seguintes ações:
   a. Limitar a estrutura de integridade à estrutura física do banco de dados (PHYSICAL_ONLY)
      i. Selecione **Limitar a estrutura de integridade à estrutura física do banco de dados (PHYSICAL_ONLY)** para limitar a verificação de integridade à estrutura física do banco de dados e detectar páginas quebradas, falhas de soma de verificação e falhas comuns de hardware que afetam o banco de dados.
   b. Suprimir todas as mensagens de informação (SEM INFOMSGS)
      i. Selecione **Suprimir todas as mensagens informativas (NO_INFOMSGS)** para suprimir todas as mensagens informativas. Selecionado por padrão.
   c. Exibir todas as mensagens de erro relatadas por objeto (ALL_ERRORMSGS)
      i. Selecione **Exibir todas as mensagens de erro relatadas por objeto (ALL_ERRORMSGS)** para exibir todos os erros relatados por objeto.
   d. Não verificar índices não agrupados (NOINDEX)
      i. Selecione **Não verificar índices não agrupados (NOINDEX)** se não quiser verificar índices não agrupados. O banco de dados SQL Server usa o Microsoft SQL Server Database Consistency Checker (DBCC) para verificar a integridade lógica e física dos objetos no banco de dados.
   e. Limite as verificações e obtenha os bloqueios em vez de usar um Snapshot de banco de dados interno (TABLOCK)
      i. Selecione **Limitar as verificações e obter os bloqueios em vez de usar uma cópia de instantâneo do banco de dados interno (TABLOCK)** para limitar as verificações e obter os bloqueios em vez de usar um instantâneo do banco de dados interno.
3. Na seção **Backup de log**, selecione **Verificar backup de log após a conclusão** para verificar o backup de log após a conclusão.
4. Na seção **Configurações do script de verificação**, insira o caminho e os argumentos do prescript ou postscript que devem ser executados antes ou depois da operação de verificação, respectivamente.

> O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_PATH.

Etapa 10: Resumo da revisão

1. Revise o resumo e selecione **Concluir**.

Crie grupos de recursos e anexe políticas para o SQL Server

Um grupo de recursos é um contêiner ao qual você adiciona recursos que deseja fazer backup e proteger juntos. Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente. Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de

proteção de dados que deseja executar.

Você pode proteger recursos individualmente sem criar um novo grupo de recursos. Você pode fazer backups no recurso protegido.

Sobre esta tarefa

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .
- Não há suporte para adicionar novos bancos de dados sem sincronização ativa do SnapMirror a um grupo de recursos existente que contém recursos com sincronização ativa do SnapMirror .
- Não há suporte para adicionar novos bancos de dados a um grupo de recursos existente no modo de failover da sincronização ativa do SnapMirror . Você pode adicionar recursos ao grupo de recursos somente no estado regular ou de failback.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** na lista **Exibir**.

   Se você adicionou recentemente um recurso ao SnapCenter, clique em **Atualizar recursos** para visualizar o recurso recém-adicionado.

3. Clique em **Novo Grupo de Recursos**.
4. Na página Nome, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Digite o nome do grupo de recursos. O nome do grupo de recursos não deve exceder 250 caracteres.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.
Use formato de nome personalizado para cópia do Snapshot	Opcional: insira um nome e formato de Snapshot personalizado. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

5. Na página Recursos, execute as seguintes etapas:
   a. Selecione o nome do host, o tipo de recurso e a instância do SQL Server nas listas suspensas para filtrar a lista de recursos.

Se você adicionou recursos recentemente, eles aparecerão na lista de Recursos Disponíveis somente depois que você atualizar sua lista de recursos.

b. Para mover recursos da seção **Recursos disponíveis** para a seção Recursos selecionados, execute uma das seguintes etapas:

- Selecione **Selecionar automaticamente todos os recursos no mesmo volume de armazenamento** para mover todos os recursos no mesmo volume para a seção Recursos selecionados.
- Selecione os recursos na seção **Recursos disponíveis** e clique na seta para a direita para movê-los para a seção **Recursos selecionados**.

6. Na página Políticas, execute as seguintes etapas:

a. Selecione uma ou mais políticas na lista suspensa.

Você também pode criar uma política clicando em * * *.

Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

b. Na seção Configurar agendamentos para políticas selecionadas, clique em * * na coluna Configurar agendamentos da política para a qual você deseja configurar o agendamento.

c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento especificando a data de início, a data de expiração e a frequência e clique em **OK**.

Você deve fazer isso para cada frequência listada na política. Os agendamentos configurados são listados na coluna Agendamentos aplicados na seção **Configurar agendamentos para políticas selecionadas**.

d. Selecione o agendador do Microsoft SQL Server.

Você também deve selecionar uma instância do agendador para associar à política de agendamento.

Se você não selecionar o agendador do Microsoft SQL Server, o padrão será o agendador do Microsoft Windows.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter . Você não deve modificar os agendamentos e renomear o trabalho de backup criado no agendador do Windows ou no agente do SQL Server.

7. Na página Verificação, execute as seguintes etapas:

a. Selecione o servidor de verificação na lista suspensa **Servidor de verificação**.

A lista inclui todos os servidores SQL adicionados no SnapCenter. Você pode selecionar vários servidores de verificação (host local ou host remoto).

A versão do servidor de verificação deve corresponder à versão e edição do servidor SQL que hospeda o banco de dados principal.

a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror e SnapVault para realizar a

verificação no armazenamento secundário.

b. Selecione a política para a qual deseja configurar seu cronograma de verificação e clique em * + *.

c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name, execute as seguintes ações:

Se você quiser…	Faça isso…
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada**.

d. Clique em **OK**.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados. Você pode revisar e editar clicando em *  * ou exclua clicando em * *.

8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

9. Revise o resumo e clique em **Concluir**.

Informações relacionadas

"Crie políticas de backup para bancos de dados SQL Server"

Crie grupos de recursos e habilite a proteção secundária para recursos do Microsoft SQL Server em sistemas ASA r2

Você deve criar o grupo de recursos para adicionar os recursos que estão nos sistemas ASA r2. Você também pode provisionar a proteção secundária ao criar o grupo de recursos.

Antes de começar

- Você deve garantir que não está adicionando recursos do ONTAP 9.x e recursos do ASA r2 ao mesmo grupo de recursos.
- Você deve garantir que não tenha um banco de dados com recursos ONTAP 9.x e recursos ASA r2.

Sobre esta tarefa

- A proteção secundária estará disponível somente se o usuário conectado estiver atribuído à função que tem o recurso **SecondaryProtection** habilitado.
- Se você habilitar a proteção secundária, o grupo de recursos será colocado no modo de manutenção durante a criação dos grupos de consistência primário e secundário. Depois que os grupos de consistência primário e secundário são criados, o grupo de recursos é retirado do modo de manutenção.

- O SnapCenter não oferece suporte à proteção secundária para um recurso clone.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:
   a. Insira um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 caracteres.

   b. Insira um ou mais rótulos no campo Tag para ajudar você a pesquisar o grupo de recursos posteriormente.

      Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.

   c. Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

      Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

   d. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

      Você deve usar exatamente o mesmo destino definido no aplicativo, incluindo o prefixo, se necessário.

4. Na página Recursos, selecione o nome do host do banco de dados na lista suspensa **Host**.

   Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos do ASA r2 na seção Recursos disponíveis e mova-os para a seção Recursos selecionados.
6. Na página Configurações do aplicativo, selecione a opção de backup.
7. Na página Políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em + .

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.
   c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e

clique em **OK**.

Onde *policy_name* é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Se a proteção secundária estiver habilitada para a política selecionada, a página Proteção Secundária será exibida e você precisará executar as seguintes etapas:
   a. Selecione o tipo de política de replicação.

      A política de replicação síncrona não é suportada.

   b. Especifique o sufixo do grupo de consistência que você deseja usar.
   c. Nos menus suspensos Cluster de destino e SVM de destino, selecione o cluster emparelhado e o SVM que você deseja usar.

      O cluster e o peering de SVM não são suportados pelo SnapCenter. Você deve usar o System Manager ou as CLIs do ONTAP para executar o peering de cluster e SVM.

Se os recursos já estiverem protegidos fora do SnapCenter, eles serão exibidos na seção Recursos Protegidos Secundários.

1. Na página Verificação, execute as seguintes etapas:
   a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para realizar a verificação no armazenamento secundário.
   b. Clique + na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política.
   c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name, execute as seguintes ações:

Se você quiser…	**Faça isso…**
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

   d. Selecione **Verificar no local secundário** para verificar seus backups no sistema de armazenamento secundário.
   e. Clique em **OK**.

      Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

2. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

3. Revise o resumo e clique em **Concluir**.

Requisitos para fazer backup de recursos SQL

Antes de fazer backup de um recurso SQL, você deve garantir que vários requisitos sejam atendidos.

- Você deve ter migrado um recurso de um sistema de armazenamento não NetApp para um sistema de armazenamento NetApp .
- Você deve ter criado uma política de backup.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.
- A operação de backup iniciada por um usuário do Active Directory (AD) falhará se a credencial da instância SQL não for atribuída ao usuário ou grupo do AD. Você deve atribuir a credencial da instância SQL ao usuário ou grupo do AD na página **Configurações** > **Acesso do usuário**.
- Você deve ter criado um grupo de recursos com uma política anexada.
- Se um grupo de recursos tiver vários bancos de dados de hosts diferentes, a operação de backup em alguns hosts poderá ser acionada tardiamente devido a problemas de rede. Você deve configurar o valor de FMaxRetryForUninitializedHosts em web.config usando o cmdlet Set-SmConfigSettings PS.

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell

Você deve criar uma conexão de máquina virtual de armazenamento (SVM) e uma credencial antes de usar cmdlets do PowerShell para executar operações de proteção de dados.

Antes de começar

- Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.
- Você deve ter as permissões necessárias na função de administrador de infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estejam em andamento.

  As instalações do plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento porque o cache do host pode não ser atualizado e o status dos bancos de dados pode ser exibido na GUI do SnapCenter como “Não disponível para backup” ou "`Não no armazenamento NetApp ".

- Os nomes dos sistemas de armazenamento devem ser exclusivos.

O SnapCenter não oferece suporte a vários sistemas de armazenamento com o mesmo nome em clusters diferentes. Cada sistema de armazenamento suportado pelo SnapCenter deve ter um nome exclusivo e um endereço IP LIF de gerenciamento exclusivo.

Passos

1. Inicie uma sessão de conexão do PowerShell Core usando o cmdlet Open-SmConnection.

   Este exemplo abre uma sessão do PowerShell:

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

2. Crie uma nova conexão com o sistema de armazenamento usando o cmdlet Add-SmStorageConnection.

   Este exemplo cria uma nova conexão de sistema de armazenamento:

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Crie uma nova credencial usando o cmdlet Add-SmCredential.

   Este exemplo cria uma nova credencial chamada FinanceAdmin com credenciais do Windows:

   ```
   PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup de recursos SQL

Se um recurso ainda não fizer parte de nenhum grupo de recursos, você poderá fazer backup do recurso na página Recursos.

Sobre esta tarefa

- Para otimizar a operação de backup, você deve criar um registro de pesquisa reversa de nomes de cluster do Windows e endereços IP no servidor DNS.
- Para autenticação de credenciais do Windows, você deve configurar suas credenciais antes de instalar os plug-ins.
- Para autenticação da instância do SQL Server, você deve adicionar a credencial após instalar os plug-ins.
- Para autenticação gMSA, você deve configurar o gMSA ao registrar o host no SnapCenter na página **Adicionar Host** ou **Modificar Host** para habilitar e usar o gMSA.
- Se o host for adicionado com o gMSA e se o gMSA tiver privilégios de login e de administrador do sistema, o gMSA poderá se conectar à instância do SQL.
  - O SnapCenter verificará se a autenticação para instâncias SQL está configurada. Se a autenticação

estiver configurada, a instância SQL será acessada usando essa credencial.

- Se a autenticação não estiver configurada, use o gMSA para verificar se o plug-in SQL está operando no momento. Se o plug-in estiver em operação, ele será usado para estabelecer uma conexão com a instância do SQL.
- A instância do SQL será acessada por meio da autenticação de credenciais do Windows quando a autenticação para instâncias do SQL não estiver configurada e o plug-in não estiver operacional.

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados**, **Instância** ou **Grupo de disponibilidade** na lista suspensa **Exibir**.

   a. Selecione o banco de dados, a instância ou o grupo de disponibilidade do qual você deseja fazer backup.

      Quando você faz um backup de uma instância, as informações sobre o último status de backup ou o registro de data e hora dessa instância não estarão disponíveis na página de recursos.

   Na exibição de topologia, não é possível diferenciar se o status do backup, o registro de data e hora ou o backup é de uma instância ou de um banco de dados.

3. Na página Recursos, marque a caixa de seleção **formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

   Por exemplo, customtext_policy_hostname ou resource_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

4. Na página Políticas, execute as seguintes tarefas:

   a. Na seção Políticas, selecione uma ou mais políticas na lista suspensa.

      Você pode criar uma política selecionando * + * para iniciar o assistente de política.

      Na seção **Configurar agendamentos para políticas selecionadas**, as políticas selecionadas são listadas.

   b. Selecione * + * na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

   c. Em **Adicionar programações para política** `policy_name` caixa de diálogo, configure a programação e selecione **OK**.

      Aqui `policy_name` é o nome da política que você selecionou.

   Os agendamentos configurados são listados na coluna **Agendamentos Aplicados**.

   a. Selecione **Usar o agendador do Microsoft SQL Server** e, em seguida, selecione a instância do agendador na lista suspensa **Instância do agendador** associada à política de agendamento.

5. Na página Verificação, execute as seguintes etapas:

   a. Selecione o servidor de verificação na lista suspensa **Servidor de verificação**.

      Você pode selecionar vários servidores de verificação (host local ou host remoto).

A versão do servidor de verificação deve ser igual ou superior à versão da edição do servidor SQL que hospeda o banco de dados primário.

a. Selecione **Carregar localizadores secundários para verificar backups no secundário** para verificar seus backups no sistema de armazenamento secundário.

b. Selecione a política para a qual deseja configurar seu cronograma de verificação e, em seguida, selecione * + *.

c. Na caixa de diálogo Adicionar agendamentos de verificação *policy_name*, execute as seguintes ações:

Se você quiser…	Faça isso…
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada**.

Se o servidor de verificação não tiver uma conexão de armazenamento, a operação de verificação falhará com o erro: Falha ao montar o disco.

d. Selecione **OK**.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

6. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

7. Revise o resumo e selecione **Concluir**.

A página de topologia do banco de dados é exibida.

8. Selecione **Fazer backup agora**.
9. Na página Backup, execute as seguintes etapas:

a. Se você aplicou várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

b. Selecione **Verificar após backup** para verificar seu backup.

c. Selecione **Backup**.

Você não deve renomear o trabalho de backup criado no agendador do Windows ou no agente do SQL Server.

Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

Um grupo de recursos implícito é criado. Você pode visualizar isso selecionando o respectivo usuário ou grupo na página Acesso do Usuário. O tipo de grupo de recursos implícito é “Recurso”.

10. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Depois que você terminar

- Nas configurações do MetroCluster , o SnapCenter pode não conseguir detectar um relacionamento de proteção após um failover.

  "Não é possível detectar o relacionamento SnapMirror ou SnapVault após failover do MetroCluster"

- Se você estiver fazendo backup de dados do aplicativo em VMDKs e o tamanho do heap Java para o SnapCenter Plug-in for VMware vSphere não for grande o suficiente, o backup poderá falhar. Para aumentar o tamanho do heap Java, localize o arquivo de script /opt/netapp/init_scripts/scvservice. Nesse roteiro, o `do_start method` O comando inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: `Java -jar -Xmx8192M -Xms4096M`.

Informações relacionadas

"Crie políticas de backup para bancos de dados SQL Server"

"As operações de backup falham com erro de conexão do MySQL devido ao atraso no TCP_TIMEOUT"

"O backup falha com erro do agendador do Windows"

"As operações de agrupamento ou de desativação de recursos falham"

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

O prompt de nome de usuário e senha é exibido.

2. Crie uma política de backup usando o cmdlet Add-SmPolicy.

Este exemplo cria uma nova política de backup com um tipo de backup SQL de FullBackup:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

Este exemplo cria uma nova política de backup com um tipo de backup do sistema de arquivos do Windows de CrashConsistent:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Descubra recursos do host usando o cmdlet Get-SmResources.

   Este exemplo descobre os recursos para o plug-in Microsoft SQL no host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

   Este exemplo descobre os recursos para sistemas de arquivos do Windows no host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Adicione um novo grupo de recursos ao SnapCenter usando o cmdlet Add-SmResourceGroup.

   Este exemplo cria um novo grupo de recursos de backup de banco de dados SQL com a política e os recursos especificados:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

   Este exemplo cria um novo grupo de recursos de backup do sistema de arquivos do Windows com a política e os recursos especificados:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Inicie uma nova tarefa de backup usando o cmdlet New-SmBackup.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Visualize o status do trabalho de backup usando o cmdlet Get-SmBackupReport.

   Este exemplo exibe um relatório de resumo de todos os trabalhos que foram executados na data especificada:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup de grupos de recursos do SQL Server

Você pode fazer backup de um grupo de recursos sob demanda na página Recursos. Se um grupo de recursos tiver uma política anexada e um agendamento configurado, os backups ocorrerão automaticamente de acordo com o agendamento.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.

   Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou selecionando e, em seguida, selecionando a tag. Você pode então selecionar para fechar o painel de filtro.

3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e selecione **Fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
   a. Se você tiver associado várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

      Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

   b. Após o backup, selecione **Verificar** para verificar o backup sob demanda.

      A opção **Verificar** na política se aplica somente a trabalhos agendados.

   c. Selecione **Backup**.
5. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Informações relacionadas

"Crie políticas de backup para bancos de dados SQL Server"

"Crie grupos de recursos e anexe políticas para o SQL Server"

"As operações de backup falham com erro de conexão do MySQL devido ao atraso no TCP_TIMEOUT"

"O backup falha com erro do agendador do Windows"

Monitore as operações de backup de recursos SQL na página Tarefas do SnapCenter

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Talvez você queira verificar o progresso para determinar quando ele foi concluído ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado correspondente das operações:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **Trabalhos**.
3. Na página Trabalhos, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de backup sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Backup**.
   d. No menu suspenso **Status**, selecione o status do backup.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione uma tarefa de backup e clique em **Detalhes** para visualizar os detalhes da tarefa.

   Embora o status do trabalho de backup seja exibido , ao clicar em detalhes do trabalho, você poderá ver que algumas das tarefas filhas da operação de backup ainda estão em andamento ou marcadas com sinais de alerta.

5. Na página Detalhes do trabalho, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Monitore as operações de proteção de dados em recursos SQL no painel Atividade

O painel Atividade exibe as cinco operações mais recentes realizadas. O painel Atividade também exibe quando a operação foi iniciada e o status da operação.

O painel Atividade exibe informações sobre operações de backup, restauração, clonagem e backup agendado.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Clique no painel Atividade para visualizar as cinco operações mais recentes.

   Quando você clica em uma das operações, os detalhes da operação são listados na página **Detalhes do trabalho**.

Cancelar o plug-in SnapCenter para operações de backup do Microsoft SQL Server

Você pode cancelar operações de backup que estejam em execução, na fila ou que não respondam. Quando você cancela uma operação de backup, o SnapCenter Server interrompe a operação e remove todos os Snapshots do armazenamento se o backup criado não estiver registrado no SnapCenter Server. Se o backup já estiver registrado no SnapCenter Server, ele não reverterá o Snapshot já criado, mesmo após o cancelamento ser acionado.

Antes de começar

- Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações de restauração.
- Você pode cancelar somente as operações de log ou backup completo que estão na fila ou em execução.
- Você não pode cancelar a operação após a verificação ter iniciado.

  Se você cancelar a operação antes da verificação, a operação será cancelada e a operação de verificação não será executada.

- Você pode cancelar uma operação de backup na página Monitor ou no painel Atividade.
- Além de usar a GUI do SnapCenter , você pode usar cmdlets do PowerShell para cancelar operações.
- O botão **Cancelar trabalho** fica desabilitado para operações que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de backup enfileiradas de outros membros enquanto estiver usando essa função.

Passos

Execute uma das seguintes ações:

Do…	Ação
Página do monitor	1. No painel de navegação esquerdo, selecione **Monitor** > **Trabalhos**. 2. Selecione o trabalho e selecione **Cancelar trabalho**.

Do…	Ação
Painel de atividades	1. Após iniciar o trabalho de backup, selecione no painel Atividade para visualizar as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes do trabalho, selecione **Cancelar trabalho**.

Resultado

A operação é cancelada e o recurso é revertido ao estado anterior. Se a operação cancelada não responder no estado de cancelamento ou execução, você deverá executar o `Cancel-SmJob -JobID <int> -Force` cmdlet para interromper forçadamente a operação de backup.

Exibir backups e clones do SQL Server na página Topologia

Ao se preparar para fazer backup ou clonar um recurso, pode ser útil visualizar uma representação gráfica de todos os backups e clones no armazenamento primário e secundário.

Sobre esta tarefa

Na página Topologia, você pode ver todos os backups e clones disponíveis para o recurso ou grupo de recursos selecionado. Você pode visualizar os detalhes desses backups e clones e selecioná-los para executar operações de proteção de dados.

Você pode revisar os seguintes ícones na exibição **Gerenciar cópias** para determinar se os backups e clones estão disponíveis no armazenamento primário ou secundário (cópias espelhadas ou cópias do Vault).

-  exibe o número de backups e clones que estão disponíveis no armazenamento primário.
-  exibe o número de backups e clones que são espelhados no armazenamento secundário usando a tecnologia SnapMirror .
-  exibe o número de backups e clones que são replicados no armazenamento secundário usando a tecnologia SnapVault .
  - O número de backups exibidos inclui os backups excluídos do armazenamento secundário.

    Por exemplo, se você criou 6 backups usando uma política para manter apenas 4 backups, o número de backups exibidos será 6.

Clones de um backup de um espelho flexível em termos de versão em um volume do tipo mirror-vault são exibidos na exibição de topologia, mas a contagem de backups de espelho na exibição de topologia não inclui o backup flexível em termos de versão.

Se você tiver um relacionamento secundário como sincronização ativa do SnapMirror (inicialmente lançado

como SnapMirror Business Continuity [SM-BC]), poderá ver os seguintes ícones adicionais:

-  O site de réplica está no ar.
-  O site de réplicas está fora do ar.
-  O espelho secundário ou o relacionamento do cofre não foram restabelecidos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso na exibição de detalhes do recurso ou na exibição de detalhes do grupo de recursos.

   Se o recurso selecionado for um banco de dados clonado, proteja o banco de dados clonado, a origem do clone será exibida na página Topologia. Clique em **Detalhes** para visualizar o backup usado para clonar.

   Se o recurso estiver protegido, a página Topologia do recurso selecionado será exibida.

4. Revise o cartão Resumo para ver um resumo do número de backups e clones disponíveis no armazenamento primário e secundário.

   A seção **Cartão de Resumo** exibe o número total de backups e clones.

   Clicar no botão **Atualizar** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clicar no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Uma programação semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo estiver distribuído em vários volumes, o tempo de expiração do SnapLock para o backup será o maior tempo de expiração do SnapLock definido para um Snapshot em um volume. O maior tempo de expiração do SnapLock é recuperado do ONTAP.

   Para sincronização ativa do SnapMirror , clicar no botão **Atualizar** atualiza o inventário de backup do SnapCenter consultando o ONTAP para sites primários e de réplica. Uma programação semanal também executa essa atividade para todos os bancos de dados que contêm o relacionamento de sincronização ativo do SnapMirror .

   - Para sincronização ativa do SnapMirror e somente para o ONTAP 9.14.1, os relacionamentos Async Mirror ou Async MirrorVault com o novo destino primário devem ser configurados manualmente após o failover. A partir do ONTAP 9.15.1, o Async Mirror ou o Async MirrorVault são configurados automaticamente para o novo destino principal.
   - Após o failover, um backup deve ser criado para que o SnapCenter esteja ciente do failover. Você pode clicar em **Atualizar** somente após um backup ter sido criado.

5. Na exibição **Gerenciar cópias**, clique em **Backups** ou **Clones** no armazenamento primário ou secundário para ver detalhes de um backup ou clone.

   Os detalhes dos backups e clones são exibidos em formato de tabela.

6. Selecione o backup na tabela e clique nos ícones de proteção de dados para executar operações de restauração, clonagem, renomeação e exclusão.

Não é possível renomear ou excluir backups que estejam no armazenamento secundário.

7. Selecione um clone da tabela e clique em **Clone Split**.
8. Se você quiser excluir um clone, selecione o clone na tabela e clique em .

Limpe a contagem de backups secundários usando cmdlets do PowerShell

Você pode usar o cmdlet Remove-SmBackup para limpar a contagem de backups para backups secundários que não têm Snapshot. Talvez você queira usar este cmdlet quando o total de Snapshots exibidos na topologia Gerenciar Cópias não corresponder à configuração de retenção de Snapshot do armazenamento secundário.

Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Limpe a contagem de backups secundários usando o parâmetro -CleanupSecondaryBackups.

   Este exemplo limpa a contagem de backups para backups secundários sem instantâneos:

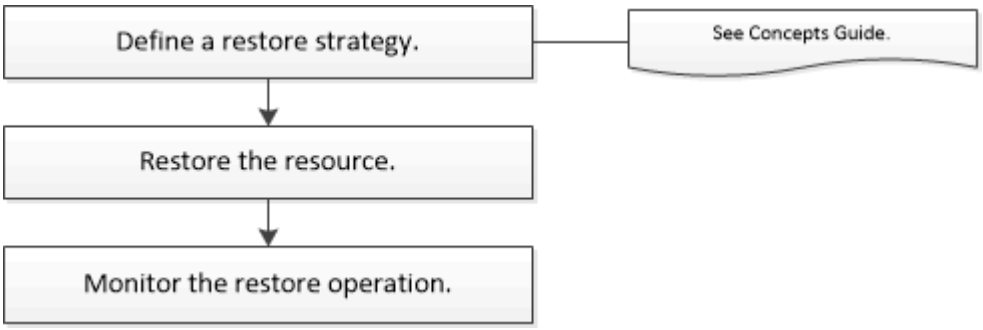
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Restaurar recursos do SQL Server

Fluxo de trabalho de restauração

Você pode usar o SnapCenter para restaurar bancos de dados do SQL Server restaurando os dados de um ou mais backups para o seu sistema de arquivos ativo e, em seguida, recuperando o banco de dados. Você também pode restaurar bancos de dados que estão em Grupos de Disponibilidade e, em seguida, adicionar os bancos de dados restaurados ao Grupo de Disponibilidade. Antes de restaurar um banco de dados do SQL Server, você deve executar várias tarefas preparatórias.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar as operações de restauração do banco de dados:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração, recuperação, verificação e clonagem. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet do SnapCenter ou consulte o "Guia de referência do cmdlet do software SnapCenter"

Encontre mais informações

"Restaurar um banco de dados SQL Server do armazenamento secundário"

"Restaurar e recuperar recursos usando cmdlets do PowerShell"

"A operação de restauração pode falhar no Windows 2008 R2"

Requisitos para restaurar um banco de dados

Antes de restaurar um banco de dados SQL Server a partir de um backup do SnapCenter Plug-in para Microsoft SQL Server, você deve garantir que vários requisitos sejam atendidos.

- A instância de destino do SQL Server deve estar online e em execução antes que você possa restaurar um banco de dados.

  Isso se aplica tanto às operações de restauração do banco de dados do usuário quanto às operações de restauração do banco de dados do sistema.

- As operações do SnapCenter agendadas para serem executadas nos dados do SQL Server que você está restaurando devem ser desabilitadas, incluindo quaisquer trabalhos agendados em servidores de gerenciamento remoto ou de verificação remota.
- Se os bancos de dados do sistema não estiverem funcionais, você deverá primeiro reconstruí-los usando um utilitário do SQL Server.
- Se você estiver instalando o plug-in, certifique-se de conceder permissões para outras funções para restaurar os backups do Grupo de Disponibilidade (AG).

  A restauração do AG falha quando uma das seguintes condições é atendida:

  - Se o plug-in for instalado pelo usuário do RBAC e um administrador tentar restaurar um backup do AG
  - Se o plug-in for instalado por um administrador e um usuário RBAC tentar restaurar um backup do AG
- Se você estiver restaurando backups de diretório de log personalizados para um host alternativo, o SnapCenter Server e o host do plug-in deverão ter a mesma versão do SnapCenter instalada.

- Você deve ter instalado o hotfix da Microsoft, KB2887595. O site de suporte da Microsoft contém mais informações sobre o KB2887595.

  "Artigo de Suporte da Microsoft 2887595: Pacote cumulativo de atualizações do Windows RT 8.1, Windows 8.1 e Windows Server 2012 R2: novembro de 2013"

- Você deve ter feito backup dos grupos de recursos ou do banco de dados.
- Se você estiver replicando Snapshots para um espelho ou cofre, o administrador do SnapCenter deverá ter atribuído a você as máquinas virtuais de armazenamento (SVMs) para os volumes de origem e de destino.

  Para obter informações sobre como os administradores atribuem recursos aos usuários, consulte as informações de instalação do SnapCenter .

- Todos os trabalhos de backup e clonagem devem ser interrompidos antes de restaurar o banco de dados.
- A operação de restauração pode atingir o tempo limite se o tamanho do banco de dados estiver em terabytes (TB).

  Você deve aumentar o valor do parâmetro RESTTimeout do SnapCenter Server para 20000000 ms executando o seguinte comando: Set-SmConfigSettings -Agent -configSettings @{"RESTTimeout" = "20000000"}. De acordo com o tamanho do banco de dados, o valor do tempo limite pode ser alterado e o valor máximo que você pode definir é 86400000 ms.

Se você quiser restaurar enquanto os bancos de dados estiverem online, a opção de restauração online deverá ser habilitada na página Restaurar.

Restaurar backups de banco de dados do SQL Server

Você pode usar o SnapCenter para restaurar bancos de dados SQL Server com backup. A restauração do banco de dados é um processo multifásico que copia todos os dados e páginas de log de um backup especificado do SQL Server para um banco de dados especificado.

Sobre esta tarefa

- Você pode restaurar os bancos de dados do SQL Server com backup em uma instância diferente do SQL Server no mesmo host onde o backup foi criado.

  Você pode usar o SnapCenter para restaurar os bancos de dados do SQL Server com backup em um caminho alternativo para não substituir uma versão de produção.

- O SnapCenter pode restaurar bancos de dados em um cluster do Windows sem deixar o grupo de clusters do SQL Server offline.
- Se ocorrer uma falha de cluster (uma operação de movimentação de grupo de clusters) durante uma operação de restauração (por exemplo, se o nó que possui os recursos ficar inativo), você deverá se reconectar à instância do SQL Server e reiniciar a operação de restauração.
- Não é possível restaurar o banco de dados quando os usuários ou os trabalhos do SQL Server Agent estiverem acessando o banco de dados.
- Não é possível restaurar bancos de dados do sistema para um caminho alternativo.
- O SCRIPTS_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCoreServiceHost.exe.Config do host do plug-in.

Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável que você use o caminho padrão por segurança.

O valor da chave pode ser exibido no swagger por meio da API: API /4.7/configsettings

Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

- A maioria dos campos nas páginas do assistente de restauração são autoexplicativos. As informações a seguir descrevem campos para os quais você pode precisar de orientação.
- Para a operação de restauração de sincronização ativa do SnapMirror , você deve selecionar o backup do local principal.
- Para políticas habilitadas para SnapLock , para ONTAP 9.12.1 e versões anteriores, se você especificar um período de bloqueio de Snapshot, os clones criados a partir de Snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock . O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

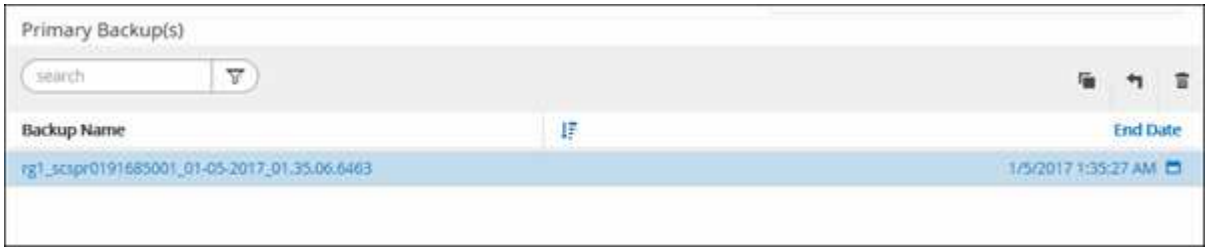
Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados ou o grupo de recursos na lista.

   A página de topologia é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** do sistema de armazenamento.
5. Selecione o backup da tabela e clique em ícone.



6. Na página Escopo de restauração, selecione uma das seguintes opções:

Opção	Descrição
Restaurar o banco de dados para o mesmo host onde o backup foi criado	Selecione esta opção se quiser restaurar o banco de dados para o mesmo servidor SQL onde os backups foram feitos.
Restaurar o banco de dados para um host alternativo	Selecione esta opção se desejar que o banco de dados seja restaurado para um servidor SQL diferente no mesmo host ou em um host diferente onde os backups são feitos. Selecione um nome de host, forneça um nome de banco de dados (opcional), selecione uma instância e especifique os caminhos de restauração. A extensão de arquivo fornecida no caminho alternativo deve ser a mesma que a extensão de arquivo do arquivo de banco de dados original. Se a opção **Restaurar o banco de dados em um host alternativo** não for exibida na página Escopo de restauração, limpe o cache do navegador.

Opção	Descrição
Restaurar o banco de dados usando arquivos de banco de dados existentes	Selecione esta opção se desejar que o banco de dados seja restaurado para um SQL Server alternativo no mesmo host ou em um host diferente onde os backups são feitos. Os arquivos de banco de dados já devem estar presentes nos caminhos de arquivo existentes fornecidos. Selecione um nome de host, forneça um nome de banco de dados (opcional), selecione uma instância e especifique os caminhos de restauração.

7. Na página Escopo de Recuperação, selecione uma das seguintes opções:

Opção	Descrição
Nenhum	Selecione **Nenhum** quando precisar restaurar apenas o backup completo, sem nenhum log.
Todos os backups de log	Selecione a operação de restauração de backup atualizada **Todos os backups de log** para restaurar todos os backups de log disponíveis após o backup completo.
Por backups de log até	Selecione **Por backups de log** para executar uma operação de restauração pontual, que restaura o banco de dados com base nos logs de backup até o log de backup com a data selecionada.
Por data específica até	Selecione **Por data específica até** para especificar a data e a hora após as quais os logs de transações não serão aplicados ao banco de dados restaurado. Esta operação de restauração pontual interrompe a restauração de entradas de log de transações que foram registradas após a data e hora especificadas.

Opção	Descrição
Usar diretório de log personalizado	Se você selecionou **Todos os backups de log**, **Por backups de log** ou **Por data específica até** e os logs estiverem localizados em um local personalizado, selecione **Usar diretório de log personalizado** e especifique o local do log. A opção **Usar diretório de log personalizado** estará disponível somente se você tiver selecionado **Restaurar o banco de dados em um host alternativo** ou **Restaurar o banco de dados usando arquivos de banco de dados existentes**. Você também pode usar o caminho compartilhado, mas certifique-se de que o caminho seja acessível ao usuário do SQL. O diretório de log personalizado não é suportado pelo banco de dados do grupo de disponibilidade.

8. Na página Pré-Operações, execute as seguintes etapas:

   a. Na página Opções de pré-restauração, selecione uma das seguintes opções:

      - Selecione **Substituir o banco de dados com o mesmo nome durante a restauração** para restaurar o banco de dados com o mesmo nome.
      - Selecione **Manter configurações de replicação do banco de dados SQL** para restaurar o banco de dados e manter as configurações de replicação existentes.
      - Selecione **Criar backup do log de transações antes da restauração** para criar um log de transações antes do início da operação de restauração.
      - Selecione **Encerrar restauração se o backup do log de transações antes da restauração falhar** para abortar a operação de restauração se o backup do log de transações falhar.

   b. Especifique scripts opcionais a serem executados antes de executar um trabalho de restauração.

      Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.

      O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_PATH.

9. Na página Post Ops, execute as seguintes etapas:

   a. Na seção Escolher estado do banco de dados após a conclusão da restauração, selecione uma das seguintes opções:

      - Selecione **Operacional, mas indisponível para restaurar logs de transações adicionais** se você estiver restaurando todos os backups necessários agora.

        Este é o comportamento padrão, que deixa o banco de dados pronto para uso, revertendo as transações não confirmadas. Você não pode restaurar logs de transações adicionais até criar

um backup.

- Selecione **Não operacional, mas disponível para restaurar logs transacionais adicionais** para deixar o banco de dados não operacional sem reverter as transações não confirmadas.

  Logs de transações adicionais podem ser restaurados. Você não pode usar o banco de dados até que ele seja recuperado.

- Selecione **Modo somente leitura, disponível para restaurar logs transacionais adicionais** para deixar o banco de dados no modo somente leitura.

  Esta opção desfaz transações não confirmadas, mas salva as ações desfeitas em um arquivo de espera para que os efeitos da recuperação possam ser revertidos.

Se a opção Desfazer diretório estiver habilitada, mais logs de transações serão restaurados. Se a operação de restauração do log de transações não for bem-sucedida, as alterações poderão ser revertidas. A documentação do SQL Server contém mais informações.

b. Especifique scripts opcionais a serem executados após executar um trabalho de restauração.

Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.

> O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_PATH.

10. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

    Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail.

11. Revise o resumo e clique em **Concluir**.
12. Monitore o processo de restauração usando a página **Monitor** > **Tarefas**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
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
```

Este exemplo exibe informações detalhadas sobre o backup de 29 de janeiro de 2015 a 3 de fevereiro de 2015:

```
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. Restaure os dados do backup usando o cmdlet Restore-SmBackup.

```
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          :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Restaurar um banco de dados SQL Server do armazenamento secundário

Você pode restaurar os bancos de dados do SQL Server com backup dos LUNs físicos (RDM, iSCSI ou FCP) em um sistema de armazenamento secundário. O recurso Restaurar é um processo multifásico que copia todos os dados e as páginas de log de um backup especificado do SQL Server que reside no sistema de armazenamento secundário para um banco de dados especificado.

Antes de começar

- Você deve ter replicado os Snapshots do sistema de armazenamento primário para o secundário.

- Você deve garantir que o SnapCenter Server e o host do plug-in consigam se conectar ao sistema de armazenamento secundário.
- A maioria dos campos nas páginas do assistente de restauração são explicados no processo básico de restauração. As informações a seguir descrevem alguns dos campos para os quais você pode precisar de orientação.

Sobre esta tarefa

Para políticas habilitadas para SnapLock , para ONTAP 9.12.1 e versões anteriores, se você especificar um período de bloqueio de Snapshot, os clones criados a partir de Snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock . O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione * SnapCenter Plug-in para SQL Server* na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista suspensa **Exibir**.
3. Selecione o banco de dados ou grupo de recursos.

   A página de topologia do banco de dados ou do grupo de recursos é exibida.
4. Na seção Gerenciar cópias, selecione **Backups** do sistema de armazenamento secundário (espelhado ou cofre).
5. Selecione o backup na lista e clique em  .
6. Na página Localização, escolha o volume de destino para restaurar o recurso selecionado.
7. Conclua o assistente de restauração, revise o resumo e clique em **Concluir**.

Se você restaurou um banco de dados para um caminho diferente que é compartilhado por outros bancos de dados, você deve executar um backup completo e uma verificação de backup para confirmar que seu banco de dados restaurado está livre de corrupção em nível físico.

Restaurar recursos usando cmdlets do PowerShell

Restaurar um backup de recursos inclui iniciar uma sessão de conexão com o SnapCenter Server, listar os backups e recuperar informações de backup, além de restaurar um backup.

Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

   ```
   PS C:\> Open-Smconnection
   ```
2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
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
```

Este exemplo exibe informações detalhadas sobre o backup de 29 de janeiro de 2015 a 3 de fevereiro de 2015:

```
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. Restaure os dados do backup usando o cmdlet Restore-SmBackup.

```
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          :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Bancos de dados do Grupo de Disponibilidade de Reseed

Reseed é uma opção para restaurar bancos de dados do Grupo de Disponibilidade (AG). Se um banco de dados secundário ficar fora de sincronia com o banco de dados primário em um AG, você poderá propagar novamente o banco de dados secundário.

Antes de começar

- Você deve ter criado um backup do banco de dados secundário do AG que deseja restaurar.
- O SnapCenter Server e o host do plug-in devem ter a mesma versão do SnapCenter instalada.

Sobre esta tarefa

- Não é possível executar a operação de nova propagação em bancos de dados primários.
- Não é possível executar uma operação de nova propagação se o banco de dados de réplica for removido do grupo de disponibilidade. Quando a réplica é removida, a operação de nova propagação falha.
- Ao executar a operação de nova propagação no banco de dados do Grupo de Disponibilidade SQL, você não deve acionar backups de log nos bancos de dados de réplica desse banco de dados do grupo de disponibilidade. Se você acionar backups de log durante uma operação de nova propagação, a operação de nova propagação falhará com a mensagem de erro O banco de dados espelho, "database_name" tem dados de log de transações insuficientes para preservar a cadeia de backup de log do banco de dados principal.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione * SnapCenter Plug-in para SQL Server* na lista.
2. Na página Recursos, selecione **Banco de dados** na lista **Exibir**.
3. Selecione o banco de dados AG secundário na lista.
4. Clique em **Reproduzir novamente**.
5. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Monitorar operações de restauração de recursos SQL

Você pode monitorar o progresso de diferentes operações de restauração do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa tomar.

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de restauração sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Restaurar**.

d. Na lista suspensa **Status**, selecione o status de restauração.

e. Clique em **Aplicar** para visualizar as operações que foram concluídas com sucesso.

4. Selecione o trabalho de restauração e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Cancelar operações de restauração de recursos SQL

Você pode cancelar trabalhos de restauração que estão na fila.

Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações de restauração.

Sobre esta tarefa

- Você pode cancelar uma operação de restauração enfileirada na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de restauração em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de restauração enfileiradas.
- O botão **Cancelar tarefa** fica desabilitado para operações de restauração que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de restauração enfileiradas de outros membros enquanto estiver usando essa função.

Etapa

Execute uma das seguintes ações:

Do…	Ação
Página do monitor	1. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. 2. Selecione o trabalho e clique em **Cancelar trabalho**.
Painel de atividades	1. Após iniciar a operação de restauração, clique em no painel Atividade para visualizar as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

Clonar recursos de banco de dados do SQL Server

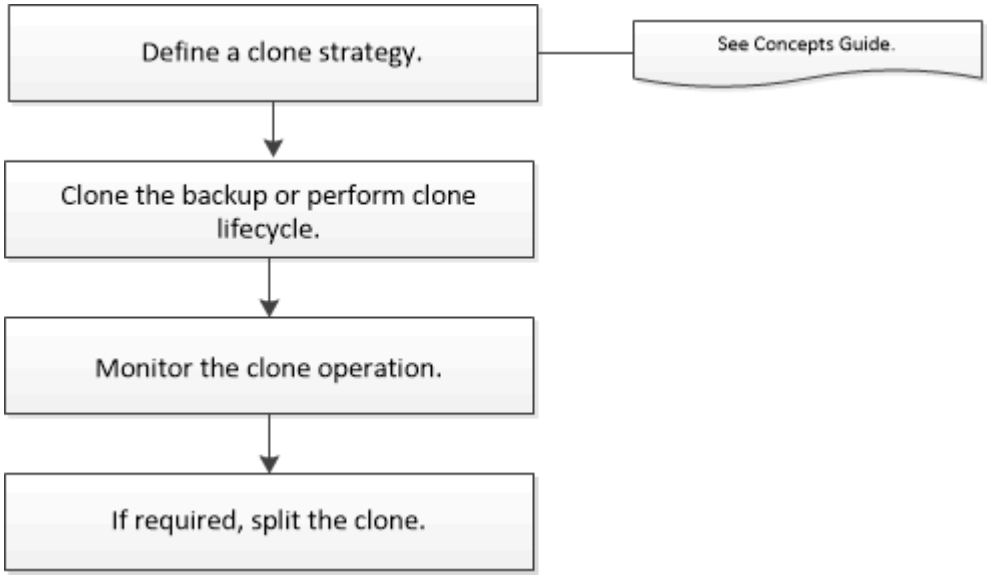
Fluxo de trabalho de clonagem

Você deve executar várias tarefas usando o SnapCenter Server antes de clonar recursos

de banco de dados de um backup. A clonagem de banco de dados é o processo de criação de uma cópia pontual de um banco de dados de produção ou de seu conjunto de backup. Você pode clonar bancos de dados para testar a funcionalidade que precisa ser implementada usando a estrutura e o conteúdo atuais do banco de dados durante os ciclos de desenvolvimento de aplicativos, para usar ferramentas de extração e manipulação de dados ao preencher data warehouses ou para recuperar dados que foram excluídos ou alterados por engano.

Uma operação de clonagem de banco de dados gera relatórios com base nos IDs de trabalho.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar as operações de clonagem:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração, recuperação, verificação e clonagem. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet do SnapCenter ou consulte o "Guia de referência do cmdlet do software SnapCenter"

Encontre mais informações

"Clonar de um backup de banco de dados SQL Server"

"Executar ciclo de vida do clone"

"A operação de clonagem pode falhar ou levar mais tempo para ser concluída com o valor TCP_TIMEOUT padrão"

Clonar de um backup de banco de dados SQL Server

Você pode usar o SnapCenter para clonar um backup de banco de dados do SQL Server. Se quiser acessar ou restaurar uma versão mais antiga dos dados, você pode clonar backups de banco de dados sob demanda.

Antes de começar

- Você deve ter se preparado para a proteção de dados concluindo tarefas como adicionar hosts, identificar recursos e criar conexões de sistema de armazenamento.

- Você deve ter feito backup de bancos de dados ou grupos de recursos.
- O tipo de proteção, como espelho, cofre ou espelho-cofre para LUN de dados e LUN de log, deve ser o mesmo para descobrir localizadores secundários durante a clonagem para um host alternativo usando backups de log.
- Se a unidade clone montada não puder ser encontrada durante uma operação de clonagem do SnapCenter , você deverá alterar o parâmetro CloneRetryTimeout do SnapCenter Server para 300.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de armazenamento (SVM).

Sobre esta tarefa

- Ao clonar para uma instância de banco de dados independente, certifique-se de que o caminho do ponto de montagem exista e que seja um disco dedicado.
- Ao clonar para uma Instância de Cluster de Failover (FCI), certifique-se de que os pontos de montagem existam, que seja um disco compartilhado e que o caminho e o FCI pertençam ao mesmo grupo de recursos SQL.
- Certifique-se de que haja apenas um vFC ou iniciador FC conectado a cada host. Isso ocorre porque o SnapCenter suporta apenas um iniciador por host.
- Se o banco de dados de origem ou a instância de destino estiver em um volume compartilhado de cluster (csv), o banco de dados clonado estará no csv.
- O SCRIPTS_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCoreServiceHost.exe.Config do host do plug-in.

  Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável que você use o caminho padrão por segurança.

  O valor da chave pode ser exibido no swagger por meio da API: API /4.7/configsettings

  Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

  Para ambientes virtuais (VMDK/RDM), certifique-se de que o ponto de montagem seja um disco dedicado.

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione * SnapCenter Plug-in para SQL Server* na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.

   A clonagem de um backup de uma instância não é suportada.

3. Selecione o banco de dados ou grupo de recursos.
4. Na página de exibição **Gerenciar cópias**, selecione o backup do sistema de armazenamento primário ou secundário (espelhado ou em cofre).
5. Selecione o backup e, em seguida, selecione *  *.
6. Na página **Opções de Clone**, execute as seguintes ações:

Para este campo…	Faça isso…
Servidor clone	Escolha um host no qual o clone deve ser criado.
Instância do clone	Escolha uma instância clone para a qual você deseja clonar o backup do banco de dados. Esta instância SQL deve estar localizada no servidor clone especificado.
Sufixo clone	Insira um sufixo que será anexado ao nome do arquivo clone para identificar que o banco de dados é um clone. Por exemplo, *db1_clone*. Se você estiver clonando para o mesmo local do banco de dados original, deverá fornecer um sufixo para diferenciar o banco de dados clonado do banco de dados original. Caso contrário, a operação falhará.

Para este campo…	Faça isso…
Atribuição automática de ponto de montagem ou Atribuição automática de ponto de montagem de volume no caminho	Escolha se deseja atribuir automaticamente um ponto de montagem ou um ponto de montagem de volume em um caminho. Atribuição automática de ponto de montagem de volume em caminho: O ponto de montagem em um caminho permite que você forneça um diretório específico. Os pontos de montagem serão criados dentro desse diretório. Antes de escolher esta opção, você deve garantir que o diretório esteja vazio. Se houver um banco de dados no diretório, o banco de dados ficará em um estado inválido após a operação de montagem.

7. Na página Logs, selecione uma das seguintes opções:

Para este campo…	Faça isso…
Nenhum	Escolha esta opção quando quiser clonar apenas o backup completo, sem nenhum log.
Todos os backups de log	Escolha esta opção para clonar todos os backups de log disponíveis datados após o backup completo.
Por backups de log até	Escolha esta opção para clonar o banco de dados com base nos logs de backup que foram criados até o log de backup com a data selecionada.
Por data específica até	Especifique a data e a hora após as quais os logs de transações não serão aplicados ao banco de dados clonado. Este clone de ponto no tempo interrompe a clonagem das entradas do log de transações que foram registradas após a data e hora especificadas.

8. Na página **Script**, insira o tempo limite do script, o caminho e os argumentos do prescript ou postscript que devem ser executados antes ou depois da operação de clonagem, respectivamente.

   Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.

   O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_PATH.

O tempo limite padrão do script é 60 segundos.

9. Na página **Notificação**, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação de clonagem realizada, selecione **Anexar relatório de trabalho**.

   > Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

   Para EMS, você pode consultar "Gerenciar coleta de dados de EMS"

10. Revise o resumo e selecione **Concluir**.
11. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Depois que você terminar

Depois que o clone for criado, você nunca deve renomeá-lo.

Informações relacionadas

"A operação de clonagem pode falhar ou levar mais tempo para ser concluída com o valor TCP_TIMEOUT padrão"

"Falha na clonagem do banco de dados da instância do cluster de failover"

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Liste os backups que podem ser clonados usando o cmdlet Get-SmBackup ou Get-SmResourceGroup.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                    BackupTime   BackupType
--------   ----------                    ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

Este exemplo exibe informações sobre um grupo de recursos especificado, seus recursos e políticas associadas:

```
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. Inicie uma operação de clonagem de um backup existente usando o cmdlet New-SmClone.

   Este exemplo cria um clone de um backup especificado com todos os logs:

```
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
```

   Este exemplo cria um clone para uma instância especificada do Microsoft SQL Server:

```
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. Visualize o status do trabalho de clonagem usando o cmdlet Get-SmCloneReport.

   Este exemplo exibe um relatório de clone para o ID do trabalho especificado:

```
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}
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Executar ciclo de vida do clone

Usando o SnapCenter, você pode criar clones de um grupo de recursos ou banco de dados. Você pode executar uma clonagem sob demanda ou agendar operações de clonagem recorrentes de um grupo de recursos ou banco de dados. Se você clonar um backup periodicamente, poderá usar o clone para desenvolver aplicativos, preencher dados ou recuperar dados.

O SnapCenter permite que você agende várias operações de clonagem para serem executadas simultaneamente em vários servidores.

Antes de começar

- Ao clonar para uma instância de banco de dados independente, certifique-se de que o caminho do ponto de montagem exista e que seja um disco dedicado.
- Ao clonar para uma Instância de Cluster de Failover (FCI), certifique-se de que os pontos de montagem existam, que seja um disco compartilhado e que o caminho e o FCI pertençam ao mesmo grupo de recursos SQL.
- Se o banco de dados de origem ou a instância de destino estiver em um volume compartilhado de cluster (csv), o banco de dados clonado estará no csv.

Para ambientes virtuais (VMDK/RDM), certifique-se de que o ponto de montagem seja um disco dedicado.

Sobre esta tarefa

- O SCRIPTS_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCoreServiceHost.exe.Config do host do plug-in.

  Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável que você use o caminho padrão por segurança.

  O valor da chave pode ser exibido no swagger por meio da API: API /4.7/configsettings

  Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

- A maioria dos campos nas páginas do assistente do ciclo de vida do Clone são autoexplicativos. As informações a seguir descrevem campos para os quais você pode precisar de orientação.
- Para o ONTAP 9.12.1 e versões anteriores, se você especificar um período de bloqueio do Snapshot, os clones criados a partir dos Snapshots à prova de violação herdarão o tempo de expiração do SnapLock . O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o grupo de recursos ou banco de dados e clique em **Clonar ciclo de vida**.
4. Na página Opções, execute as seguintes ações:

Para este campo…	Faça isso…
Nome do trabalho de clonagem	Especifique o nome do trabalho do ciclo de vida do clone que ajuda a monitorar e modificar o trabalho do ciclo de vida do clone.
Servidor clone	Escolha o host no qual o clone deve ser colocado.
Instância do clone	Escolha a instância clone para a qual você deseja clonar o banco de dados. Esta instância SQL deve estar localizada no servidor clone especificado.

Para este campo…	Faça isso…
Sufixo clone	Insira um sufixo que será anexado ao banco de dados clone para identificar que é um clone. Cada instância SQL usada para criar um grupo de recursos de clone deve ter um nome de banco de dados exclusivo. Por exemplo, se o grupo de recursos clone contiver um banco de dados de origem “db1” de uma instância SQL “inst1”, e se “db1” for clonado para “inst1”, o nome do banco de dados clone deverá ser “db1*clone”. “*clone” é um sufixo obrigatório definido pelo usuário porque o banco de dados é clonado para a mesma instância. Se “db1” for clonado para a instância SQL “inst2”, o nome do banco de dados clonado poderá permanecer “db1” (o sufixo é opcional) porque o banco de dados será clonado para uma instância diferente.
Atribuição automática de ponto de montagem ou Atribuição automática de ponto de montagem de volume no caminho	Escolha se deseja atribuir automaticamente um ponto de montagem ou um ponto de montagem de volume em um caminho. Escolher atribuir automaticamente um ponto de montagem de volume em um caminho permite que você forneça um diretório específico. Os pontos de montagem serão criados dentro desse diretório. Antes de escolher esta opção, você deve garantir que o diretório esteja vazio. Se houver um banco de dados no diretório, o banco de dados estará em um estado inválido após a operação de montagem.

5. Na página Localização, selecione um local de armazenamento para criar um clone.
6. Na página Script, insira o caminho e os argumentos do prescript ou postscript que devem ser executados antes ou depois da operação de clonagem, respectivamente.

   Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.

   > O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_PATH.

   O tempo limite padrão do script é 60 segundos.

7. Na página Agendar, execute uma das seguintes ações:
   - Selecione **Executar agora** se quiser executar o trabalho de clonagem imediatamente.
   - Selecione **Configurar agendamento** quando quiser determinar com que frequência a operação de clonagem deve ocorrer, quando o agendamento de clonagem deve começar, em que dia a operação de clonagem deve ocorrer, quando o agendamento deve expirar e se os clones devem ser excluídos após o agendamento expirar.
8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação de clonagem realizada, selecione **Anexar relatório de trabalho**.

Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

Para EMS, você pode consultar "Gerenciar coleta de dados de EMS"

9. Revise o resumo e clique em **Concluir**.

Você deve monitorar o processo de clonagem usando a página **Monitor** > **Jobs**.

Monitorar operações de clonagem de banco de dados SQL

Você pode monitorar o progresso das operações de clonagem do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente operações de clonagem sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione o trabalho de clonagem e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página Detalhes do trabalho, clique em **Exibir registros**.

Cancelar operações de clonagem de recursos SQL

Você pode cancelar operações de clonagem que estão na fila.

Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar operações de clonagem.

Sobre esta tarefa

- Você pode cancelar uma operação de clone enfileirada na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de clonagem em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de clonagem enfileiradas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de clonagem enfileiradas de outros membros enquanto estiver usando essa função.

Etapa

Execute uma das seguintes ações:

Do…	Ação
Página do monitor	1. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. 2. Selecione a operação e clique em **Cancelar trabalho**.
Painel de atividades	1. Após iniciar a operação de clonagem, clique em no painel Atividade para visualizar as cinco operações mais recentes. 2. Selecione a operação. 3. Na página **Detalhes do trabalho**, clique em **Cancelar trabalho**.

Dividir um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido se torna independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clone em um clone intermediário.

  Por exemplo, depois de criar o clone1 a partir de um backup de banco de dados, você pode criar um backup do clone1 e então clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e você não pode executar a operação de divisão de clone no clone1. No entanto, você pode executar a operação de divisão de clone no clone2.

  Após dividir o clone2, você pode executar a operação de divisão do clone no clone1 porque o clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e os trabalhos de clonagem do clone são excluídos.
- Para obter informações sobre as operações de divisão de volume do FlexClone , consulte "Dividir um volume FlexClone de seu volume pai" .
- Certifique-se de que o volume ou agregado no sistema de armazenamento esteja online.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página **Recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicações de banco de dados	Selecione **Banco de dados** na lista Exibir.
Para sistemas de arquivos	Selecione **Caminho** na lista Exibir.

3. Selecione o recurso apropriado na lista.

   A página de topologia de recursos é exibida.

4. Na exibição **Gerenciar cópias**, selecione o recurso clonado (por exemplo, o banco de dados ou LUN) e clique em *  *.
5. Revise o tamanho estimado do clone que será dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

   A operação de divisão do clone para de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clone e, em seguida, tentar novamente a operação de divisão de clone.

   Se você quiser um tempo de pesquisa maior ou menor para verificar se o clone está dividido ou não, você pode alterar o valor do parâmetro *CloneSplitStatusCheckPollTime* no arquivo *SMCoreServiceHost.exe.config* para definir o intervalo de tempo para o SMCore pesquisar o status da operação de divisão do clone. O valor está em milissegundos e o valor padrão é 5 minutos.

   Por exemplo:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   A operação de início da divisão do clone falha se um backup, uma restauração ou outra divisão do clone estiver em andamento. Você deve reiniciar a operação de divisão do clone somente após a conclusão das operações em execução.

Informações relacionadas

"O clone ou a verificação do SnapCenter falham com o agregado inexistente"

Proteja bancos de dados SAP HANA

Plug-in SnapCenter para bancos de dados SAP HANA

Visão geral do plug-in SnapCenter para banco de dados SAP HANA

O plug-in SnapCenter para banco de dados SAP HANA é um componente do lado do host do software NetApp SnapCenter software que permite o gerenciamento de proteção de dados com reconhecimento de aplicativo de bancos de dados SAP HANA. O plug-in para banco de dados SAP HANA automatiza o backup, a restauração e a clonagem de bancos de dados SAP HANA no seu ambiente SnapCenter .

O SnapCenter oferece suporte a contêineres de banco de dados de contêiner único e multilocatário (MDC). Você pode usar o plug-in para banco de dados SAP HANA em ambientes Windows e Linux. O plug-in que não está instalado no host do banco de dados HANA é conhecido como plug-in de host centralizado. O plug-in de host centralizado pode gerenciar vários bancos de dados HANA em hosts diferentes.

Quando o plug-in para banco de dados SAP HANA estiver instalado, você poderá usar o SnapCenter com a tecnologia NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume. Você também pode usar o plug-in com a tecnologia NetApp SnapVault para executar a replicação de backup de disco para disco para conformidade com os padrões.

O plug-in para banco de dados SAP HANA oferece suporte à sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC]), que permite que os serviços empresariais continuem operando mesmo durante uma falha completa do site, permitindo que os aplicativos façam failover de forma transparente usando uma cópia secundária. Não é necessária intervenção manual nem script adicional para acionar um failover com a sincronização ativa do SnapMirror .

O que você pode fazer usando o plug-in SnapCenter para banco de dados SAP HANA

Ao instalar o Plug-in para Banco de Dados SAP HANA em seu ambiente, você pode usar o SnapCenter para fazer backup, restaurar e clonar bancos de dados SAP HANA e seus recursos. Você também pode executar tarefas de suporte a essas operações.

- Adicionar bancos de dados.
- Crie backups.
- Restaurar a partir de backups.
- Clonar backups.
- Agende operações de backup.
- Monitore operações de backup, restauração e clonagem.
- Visualize relatórios de operações de backup, restauração e clonagem.

Recursos do plug-in SnapCenter para banco de dados SAP HANA

O SnapCenter integra-se ao aplicativo plug-in e às tecnologias NetApp no sistema de armazenamento. Para trabalhar com o Plug-in para Banco de Dados SAP HANA, use a

interface gráfica do usuário do SnapCenter .

- **Interface gráfica de usuário unificada**

  A interface do SnapCenter fornece padronização e consistência entre plug-ins e ambientes. A interface do SnapCenter permite que você conclua operações consistentes de backup, restauração e clonagem em plug-ins, use relatórios centralizados, use visualizações de painel rápidas, configure o controle de acesso baseado em função (RBAC) e monitore trabalhos em todos os plug-ins.

- **Administração central automatizada**

  Você pode agendar operações de backup, configurar retenção de backup baseada em políticas e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- **Tecnologia de cópia NetApp Snapshot não disruptiva**

  O SnapCenter usa a tecnologia NetApp Snapshot com o plug-in para banco de dados SAP HANA para fazer backup de recursos.

O uso do plug-in para banco de dados SAP HANA também oferece os seguintes benefícios:

- Suporte para fluxos de trabalho de backup, restauração e clonagem
- Segurança com suporte RBAC e delegação centralizada de funções

  Você também pode definir as credenciais para que os usuários autorizados do SnapCenter tenham permissões no nível do aplicativo.

- Criação de cópias de recursos com eficiência de espaço e em um determinado momento para testes ou extração de dados usando a tecnologia NetApp FlexClone

  Uma licença FlexClone é necessária no sistema de armazenamento onde você deseja criar o clone.

- Suporte para o recurso Snapshot do grupo de consistência (CG) do ONTAP como parte da criação de backups.
- Capacidade de executar vários backups simultaneamente em vários hosts de recursos

  Em uma única operação, os Snapshots são consolidados quando recursos em um único host compartilham o mesmo volume.

- Capacidade de criar Snapshots usando comandos externos.
- Suporte para backup baseado em arquivo.
- Suporte para Linux LVM no sistema de arquivos XFS.

Tipos de armazenamento suportados pelo plug-in SnapCenter para banco de dados SAP HANA

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e virtuais (VMs). Você deve verificar o suporte para seu tipo de armazenamento antes de instalar o SnapCenter Plug-in para o banco de dados SAP HANA.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados por FC • LUNs conectados por iSCSI • Volumes conectados ao NFS
VMware ESXi	• LUNs RDM conectados por um FC ou iSCSI ESXi HBAA varredura de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluída porque o SnapCenter verifica todos os adaptadores de barramento de host presentes no host. Você pode editar o arquivo **LinuxConfig.pm** localizado em */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* para definir o valor do parâmetro **SCSI_HOSTS_OPTIMIZED_RESCAN** como 1 para verificar novamente apenas os HBAs listados em HBA_DRIVER_NAMES. • LUNs iSCSI conectados diretamente ao sistema convidado pelo iniciador iSCSI • VMDKs em armazenamentos de dados NFS • VMDKs em VMFS criados • Volumes NFS conectados diretamente ao sistema convidado • Armazenamentos de dados vVol em NFS e SAN O armazenamento de dados vVol só pode ser provisionado com o ONTAP Tools para VMware vSphere.

Privilégios mínimos do ONTAP necessários para o plug-in SAP HANA

Os privilégios mínimos do ONTAP necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos de acesso total: privilégios mínimos necessários para ONTAP 9.12.1 e posterior
  - evento generate-autosupport-log
  - histórico de trabalho mostrar
  - parada de trabalho
  - lua
  - lun criar
  - lun criar
  - lun criar

- lun delete
- lun igroup adicionar
- lun igroup criar
- lun igroup excluir
- renomear lun igroup
- renomear lun igroup
- show do lun igroup
- mapeamento lun add-reporting-nodes
- criação de mapeamento lun
- exclusão de mapeamento lun
- mapeamento lun remove-reporting-nodes
- show de mapeamento lunar
- lun modificar
- volume de entrada lun
- lua offline
- lua online
- lun persistente-reserva clara
- redimensionamento de lun
- série lun
- show de lua
- política de adição de regra do snapmirror
- regra de modificação de política do snapmirror
- política de remoção do snapmirror
- política do snapmirror mostrar
- restauração do snapmirror
- show de espelhos instantâneos
- histórico de exibição do snapmirror
- atualização do snapmirror
- atualização do snapmirror-ls-set
- lista-destinos do snapmirror
- versão
- criação de clone de volume
- show de clones de volume
- volume clone split start
- volume clone divisão parada
- volume criar
- destruição de volume

    - clone de arquivo de volume criar
    - arquivo de volume mostrar-uso-do-disco
    - volume offline
    - volume on-line
    - modificação de volume
    - volume qtree criar
    - volume qtree delete
    - volume qtree modificar
    - volume qtree mostrar
    - restrição de volume
    - show de volume
    - criação de instantâneo de volume
    - exclusão de instantâneo de volume
    - modificação de instantâneo de volume
    - instantâneo de volume modificar-tempo-de-expiração-do-snaplock
    - renomeação de instantâneo de volume
    - restauração de instantâneo de volume
    - arquivo de restauração de instantâneo de volume
    - exibição de instantâneo de volume
    - desmontagem de volume
    - cifs do vserver
    - vserver cifs compartilhar criar
    - vserver cifs compartilhar excluir
    - vserver cifs shadowcopy mostrar
    - vserver cifs compartilhar mostrar
    - vserver cifs mostrar
    - política de exportação do vserver
    - criação de política de exportação do vserver
    - exclusão da política de exportação do vserver
    - criação de regra de política de exportação do vserver
    - mostrar regra de política de exportação do vserver
    - mostrar política de exportação do vserver
    - vserver iscsi
    - mostrar conexão iscsi do vserver
    - vserver mostrar
- Comandos somente leitura: privilégios mínimos necessários para ONTAP 8.3.0 e posterior
    - interface de rede

- exibição de interface de rede
- vserver

Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para bancos de dados SAP HANA

Você pode usar um plug-in SnapCenter com a tecnologia ONTAP SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia ONTAP SnapVault para executar replicação de backup de disco para disco para conformidade com padrões e outros propósitos relacionados à governança. Antes de executar essas tarefas, você deve configurar um relacionamento de proteção de dados entre os volumes de origem e destino e inicializar o relacionamento.

O SnapCenter executa as atualizações no SnapMirror e no SnapVault após concluir a operação Snapshot. As atualizações do SnapMirror e do SnapVault são executadas como parte do trabalho do SnapCenter ; não crie uma programação ONTAP separada.

Se você estiver acessando o SnapCenter a partir de um produto NetApp SnapManager e estiver satisfeito com os relacionamentos de proteção de dados configurados, pode pular esta seção.

Um relacionamento de proteção de dados replica dados do armazenamento primário (o volume de origem) para o armazenamento secundário (o volume de destino). Quando você inicializa o relacionamento, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não oferece suporte a relacionamentos em cascata entre volumes SnapMirror e SnapVault (**Primário** > **Espelho** > **Cofre**). Você deve usar relacionamentos fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis em termos de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis em termos de versão e como configurá-los, consulte "Documentação do ONTAP" .

Estratégia de backup para bancos de dados SAP HANA

Definir uma estratégia de backup para bancos de dados SAP HANA

Definir uma estratégia de backup antes de criar suas tarefas de backup ajuda você a ter os backups necessários para restaurar ou clonar seus recursos com sucesso. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (RTO) e objetivo de ponto de recuperação (RPO) determinam em grande parte sua estratégia de backup.

Sobre esta tarefa

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. RTO é o tempo em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. SLA, RTO e RPO contribuem para a estratégia de proteção de dados.

Passos

1. Determine quando você deve fazer backup dos seus recursos.
2. Decida quantos trabalhos de backup você precisa.
3. Decida como nomear seus backups.
4. Decida se você deseja criar uma política baseada em cópia de Snapshot para fazer backup de Snapshots consistentes com o aplicativo do banco de dados.
5. Decida se você deseja verificar a integridade do banco de dados.
6. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção de longo prazo.
7. Determine o período de retenção dos Snapshots no sistema de armazenamento de origem e no destino do SnapMirror .
8. Determine se você deseja executar algum comando antes ou depois da operação de backup e forneça uma prescrição ou pós-escrito.

Descoberta automática de recursos no host Linux

Os recursos são bancos de dados SAP HANA e volumes não relacionados a dados no host Linux que são gerenciados pelo SnapCenter. Após instalar o plug-in SnapCenter Plug-in para banco de dados SAP HANA, os bancos de dados SAP HANA naquele host Linux são descobertos automaticamente e exibidos na página Recursos.

A descoberta automática é suportada pelos seguintes recursos do SAP HANA:

- Recipientes individuais

  Após instalar ou atualizar o plug-in, os recursos de contêiner único localizados em um plug-in de host centralizado continuarão como recursos adicionados manualmente.

  Após instalar ou atualizar o plug-in, os bancos de dados SAP HANA são descobertos automaticamente apenas nos hosts SAP HANA Linux, que são registrados diretamente no SnapCenter.

- Contêiner de banco de dados multilocatário (MDC)

  Após instalar ou atualizar o plug-in, os recursos do MDC localizados em um plug-in de host centralizado continuarão como recursos adicionados manualmente.

  Você deve continuar adicionando manualmente os recursos do MDC no plug-in do host centralizado após atualizar para o SnapCenter 4.3.

  Para hosts SAP HANA Linux registrados diretamente no SnapCenter, a instalação ou atualização do plug-in acionará uma descoberta automática de recursos no host. Após atualizar o plug-in, para cada recurso MDC localizado no host do plug-in, outro recurso MDC será descoberto automaticamente com um formato GUID diferente e registrado no SnapCenter. O novo recurso estará em estado bloqueado.

  Por exemplo, no SnapCenter 4.2, se o recurso E90 MDC estava localizado no host do plug-in e registrado manualmente, após a atualização para o SnapCenter 4.3, outro recurso E90 MDC com um GUID diferente será descoberto e registrado no SnapCenter.

A descoberta automática não é suportada para as seguintes configurações:

- Layouts RDM e VMDK

Caso os recursos acima sejam descobertos, as operações de proteção de dados não serão suportadas nesses recursos.

- Configuração de múltiplos hosts do HANA
- Várias instâncias no mesmo host
- Replicação do sistema HANA com escalonamento multicamadas
- Ambiente de replicação em cascata no modo de replicação do sistema

Tipo de backups suportados

O tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter oferece suporte aos tipos de backup baseado em arquivo e backup baseado em cópia de instantâneo para bancos de dados SAP HANA.

Backup baseado em arquivo

Backups baseados em arquivo verificam a integridade do banco de dados. Você pode agendar a operação de backup baseada em arquivo para ocorrer em intervalos específicos. Somente locatários ativos são copiados. Não é possível restaurar e clonar backups baseados em arquivo do SnapCenter.

Backup baseado em cópia instantânea

Os backups baseados em cópias de instantâneo aproveitam a tecnologia NetApp Snapshot para criar cópias on-line somente leitura dos volumes nos quais os bancos de dados SAP HANA residem.

Como o plug-in SnapCenter para banco de dados SAP HANA usa instantâneos de grupo de consistência

Você pode usar o plug-in para criar instantâneos de grupos de consistência para grupos de recursos. Um grupo de consistência é um contêiner que pode abrigar vários volumes para que você possa gerenciá-los como uma única entidade. Um grupo de consistência são instantâneos simultâneos de vários volumes, fornecendo cópias consistentes de um grupo de volumes.

Você também pode especificar o tempo de espera para que o controlador de armazenamento agrupe Snapshots de forma consistente. As opções de tempo de espera disponíveis são **Urgente**, **Médio** e **Relaxado**. Você também pode habilitar ou desabilitar a sincronização do Write Anywhere File Layout (WAFL) durante a operação consistente do Snapshot do grupo. A sincronização do WAFL melhora o desempenho de um Snapshot de grupo de consistência.

Como o SnapCenter gerencia a manutenção de backups de log e dados

O SnapCenter gerencia a manutenção de backups de log e dados nos níveis do sistema de armazenamento e do sistema de arquivos, e dentro do catálogo de backup do SAP HANA.

Os snapshots no armazenamento primário ou secundário e suas entradas correspondentes no catálogo do SAP HANA são excluídos com base nas configurações de retenção. As entradas do catálogo SAP HANA também são excluídas durante o backup e a exclusão do grupo de recursos.

Considerações para determinar agendamentos de backup para banco de dados SAP HANA

O fator mais crítico na determinação de um cronograma de backup é a taxa de alteração do recurso. Você pode fazer backup de um recurso muito utilizado a cada hora, enquanto pode fazer backup de um recurso raramente utilizado uma vez por dia. Outros fatores incluem a importância do recurso para sua organização, seu acordo de nível de serviço (SLA) e seu objetivo de ponto de recuperação (RPO).

Os agendamentos de backup têm duas partes, conforme a seguir:

- Frequência de backup (com que frequência os backups devem ser realizados)

  A frequência de backup, também chamada de tipo de agendamento para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como horária, diária, semanal ou mensal.

- Agendamentos de backup (exatamente quando os backups devem ser executados

  Os agendamentos de backup fazem parte de uma configuração de recurso ou grupo de recursos. Por exemplo, se você tiver um grupo de recursos com uma política configurada para backups semanais, poderá configurar o agendamento para fazer backup todas as quintas-feiras às 22h.

Número de trabalhos de backup necessários para bancos de dados SAP HANA

Os fatores que determinam o número de tarefas de backup necessárias incluem o tamanho do recurso, o número de volumes usados, a taxa de alteração do recurso e seu Contrato de Nível de Serviço (SLA).

Convenções de nomenclatura de backup para plug-in para bancos de dados SAP HANA

Você pode usar a convenção de nomenclatura padrão do Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um registro de data e hora aos nomes de instantâneos que ajuda a identificar quando as cópias foram criadas.

O Snapshot usa a seguinte convenção de nomenclatura padrão:

```
resourcegroupname_hostname_timestamp
```

Você deve nomear seus grupos de recursos de backup logicamente, como no exemplo a seguir:

```
dts1_mach1x88_03-12-2015_23.17.26
```

Neste exemplo, os elementos de sintaxe têm os seguintes significados:

- *dts1* é o nome do grupo de recursos.
- *mach1x88* é o nome do host.
- *03-12-2015_23.17.26* é a data e o registro de data e hora.

Como alternativa, você pode especificar o formato do nome do Snapshot ao proteger recursos ou grupos de recursos selecionando **Usar formato de nome personalizado para cópia do Snapshot**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do registro de data e hora é adicionado ao nome do Snapshot.

Estratégia de restauração e recuperação para bancos de dados SAP HANA

Definir uma estratégia de restauração e recuperação para recursos SAP HANA

Você deve definir uma estratégia antes de restaurar e recuperar seu banco de dados para que possa executar operações de restauração e recuperação com sucesso.

Passos

1. Determinar as estratégias de restauração suportadas para recursos SAP HANA adicionados manualmente
2. Determinar as estratégias de restauração suportadas para bancos de dados SAP HANA descobertos automaticamente
3. Decida o tipo de operações de recuperação que você deseja executar.

Tipos de estratégias de restauração suportadas para recursos SAP HANA adicionados manualmente

Você deve definir uma estratégia antes de poder executar com sucesso operações de restauração usando o SnapCenter. Há dois tipos de estratégias de restauração para recursos SAP HANA adicionados manualmente. Não é possível recuperar recursos do SAP HANA adicionados manualmente.

Não é possível recuperar recursos do SAP HANA adicionados manualmente.

Restauração completa de recursos

- Restaura todos os volumes, qtrees e LUNs de um recurso

Se o recurso contiver volumes ou qtrees, os Snapshots tirados após o Snapshot selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

Restauração em nível de arquivo

- Restaura arquivos de volumes, qtrees ou diretórios
- Restaura apenas os LUNs selecionados

Tipos de estratégias de restauração com suporte para bancos de dados SAP HANA descobertos automaticamente

Você deve definir uma estratégia antes de poder executar com sucesso operações de restauração usando o SnapCenter. Há dois tipos de estratégias de restauração para bancos de dados SAP HANA descobertos automaticamente.

Restauração completa de recursos

- Restaura todos os volumes, qtrees e LUNs de um recurso
  - A opção **Reverter volume** deve ser selecionada para restaurar o volume inteiro.

> Se o recurso contiver volumes ou qtrees, os Snapshots tirados após o Snapshot selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

Banco de dados de inquilinos

- Restaura o banco de dados do locatário

Se a opção **Banco de dados de locatários** for selecionada, os scripts de recuperação do HANA Studio ou do HANA externos ao SnapCenter deverão ser usados para executar a operação de recuperação.

Tipos de operações de restauração para bancos de dados SAP HANA descobertos automaticamente

O SnapCenter oferece suporte a tipos de restauração SnapRestore baseado em volume (VBSR), SnapRestore de arquivo único e conectar e copiar para bancos de dados SAP HANA descobertos automaticamente.

O SnapRestore baseado em volume (VBSR) é executado em ambientes NFS para os seguintes cenários:

- Quando o backup selecionado para restauração for feito em versões anteriores ao SnapCenter 4.3 e somente se a opção **Recurso Completo** estiver selecionada
- Quando o backup selecionado para restauração é feito no SnapCenter 4.3 e se a opção **Volume Revert** estiver selecionada

O Single File SnapRestore é executado em ambientes NFS para os seguintes cenários:

- Quando o backup selecionado para restauração é feito no SnapCenter 4.3 e se apenas a opção **Recurso Completo** é selecionada
- Para contêineres de banco de dados multilocatário (MDC), quando o backup selecionado para restauração é feito no SnapCenter 4.3 e a opção **Banco de dados locatário** é selecionada
- Quando o backup selecionado for de um local secundário do SnapMirror ou SnapVault e a opção **Recurso Completo** for selecionada

O Single File SnapRestore é executado em ambientes SAN para os seguintes cenários:

- Quando os backups são feitos em versões anteriores ao SnapCenter 4.3 e somente se a opção **Recurso Completo** estiver selecionada
- Quando os backups são feitos no SnapCenter 4.3, e somente se a opção **Recurso Completo** estiver selecionada
- Quando o backup é selecionado de um local secundário do SnapMirror ou SnapVault e a opção **Recurso Completo** é selecionada

A restauração baseada em conectar e copiar é executada em ambientes SAN para o seguinte cenário:

- Para o MDC, quando o backup selecionado para restauração é feito no SnapCenter 4.3 e a opção **Banco de Dados de Locatários** é selecionada

> As opções **Recurso Completo**, **Reversão de Volume** e **Banco de Dados de Locatários** estão disponíveis na página Escopo de Restauração.

Tipos de operações de recuperação suportadas para bancos de dados SAP HANA

O SnapCenter permite que você execute diferentes tipos de operações de recuperação para bancos de dados SAP HANA.

- Recuperar o banco de dados até o estado mais recente
- Recuperar o banco de dados até um ponto específico no tempo

  Você deve especificar a data e a hora da recuperação.

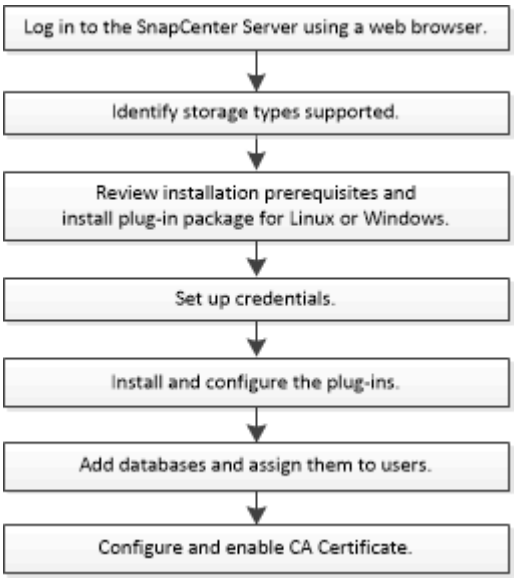
- Recuperar o banco de dados até um backup de dados específico

O SnapCenter também oferece a opção Sem recuperação para bancos de dados SAP HANA.

Prepare-se para instalar o plug-in SnapCenter para banco de dados SAP HANA

Fluxo de trabalho de instalação do plug-in SnapCenter para banco de dados SAP HANA

Você deve instalar e configurar o SnapCenter Plug-in para banco de dados SAP HANA se quiser proteger bancos de dados SAP HANA.



Pré-requisitos para adicionar hosts e instalar o plug-in SnapCenter para banco de dados SAP HANA

Antes de adicionar um host e instalar os pacotes de plug-in, você deve concluir todos os requisitos. O plug-in SnapCenter para banco de dados SAP HANA está disponível em ambientes Windows e Linux.

- Você deve ter instalado o Java 11 no seu host.

  O IBM Java não é suportado em hosts Windows e Linux.

- Você deve ter instalado o terminal interativo do banco de dados SAP HANA (cliente HDBSQL) no host.
- No Windows, o serviço do criador de plug-ins deve ser executado usando o usuário do Windows “LocalSystem”, que é o comportamento padrão quando o plug-in para banco de dados SAP HANA é instalado como administrador de domínio.
- No Windows, as chaves de armazenamento do usuário devem ser criadas como usuário SYSTEM.
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host. O plug-in SnapCenter para Microsoft Windows será implantado por padrão com o plug-in SAP HANA em hosts Windows.
- Para o host Linux, as chaves do HDB Secure User Store são acessadas como usuário do sistema operacional HDBSQL.
- O SnapCenter Server deve ter acesso à porta 8145 ou personalizada do host do Plug-in para banco de dados SAP HANA.

Hosts do Windows

- Você deve ter um usuário de domínio com privilégios de administrador local e permissões de login local no host remoto.
- Ao instalar o Plug-in para Banco de Dados SAP HANA em um host Windows, o SnapCenter Plug-in para Microsoft Windows é instalado automaticamente.
- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 no seu host Windows.

  "Baixe JAVA para todos os sistemas operacionais"

  "Ferramenta de Matriz de Interoperabilidade da NetApp"

Hosts Linux

- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 no seu host Linux.

  "Baixe JAVA para todos os sistemas operacionais"

  "Ferramenta de Matriz de Interoperabilidade da NetApp"

- Para bancos de dados SAP HANA em execução em um host Linux, ao instalar o Plug-in para Banco de Dados SAP HANA, o SnapCenter Plug-in para UNIX é instalado automaticamente.

- Você deve ter **bash** como o shell padrão para instalação de plug-ins.

Comandos suplementares

Para executar um comando suplementar no SnapCenter Plug-in para SAP HANA, você deve incluí-lo no arquivo *allowed_commands.config*.

- Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Para permitir comandos suplementares no host do plug-in, abra o arquivo *allowed_commands.config* em um editor. Digite cada comando em uma linha separada e os comandos não diferenciam maiúsculas de minúsculas. Certifique-se de especificar o caminho totalmente qualificado e coloque-o entre aspas (") se ele contiver espaços.

Por exemplo:

comando: montar

comando: umount

comando: "C:\Arquivos de Programas\ NetApp\Comandos do SnapCreator\sdcli.exe"

comando: myscript.bat

Se o arquivo *allowed_commands.config* não estiver presente, os comandos ou a execução do script serão bloqueados e o fluxo de trabalho falhará com o seguinte erro:

"[/mnt/mount -a] execução não permitida. Autorize adicionando o comando no arquivo %s no host do plugin."

Se o comando ou script não estiver presente no *allowed_commands.config*, a execução do comando ou script será bloqueada e o fluxo de trabalho falhará com o seguinte erro:

"[/mnt/mount -a] execução não permitida. Autorize adicionando o comando no arquivo %s no host do plugin."

Você não deve usar uma entrada curinga (*) para permitir todos os comandos.

Configurar privilégios sudo para usuários não root para host Linux

O SnapCenter 2.0 e versões posteriores permitem que um usuário não root instale o Pacote de plug-ins do SnapCenter para Linux e inicie o processo de plug-in. Os processos do plug-in serão executados como um usuário não root efetivo. Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se a umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro dela tenham permissão de 555. Caso contrário, a instalação do plug-in poderá falhar.
- Para o usuário não root, certifique-se de que o nome do usuário não root e o nome do grupo do usuário sejam os mesmos.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos do código de autenticação de

mensagens: MACs hmac-sha2-256 e MACs hmac-sha2-512.

Reinicie o serviço sshd após atualizar o arquivo de configuração.

Exemplo:

```
#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
```

Sobre esta tarefa

Você deve configurar privilégios sudo para que o usuário não root forneça acesso aos seguintes caminhos:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /localização_personalizada/ NetApp/snapcenter/spl/instalação/plugins/desinstalação
- /localização_personalizada/ NetApp/snapcenter/spl/bin/spl

Passos

1. Efetue login no host Linux no qual você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
2. Adicione as seguintes linhas ao arquivo /etc/sudoers usando o utilitário visudo Linux.

```
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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Se você tiver uma configuração RAC, junto com os outros comandos permitidos, você deve adicionar o seguinte ao arquivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Você pode obter o valor de *crs_home* do arquivo */etc/oracle/olr.loc*.

LINUX_USER é o nome do usuário não root que você criou.

Você pode obter o *checksum_value* do arquivo **sc_unix_plugins_checksum.txt**, localizado em:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Linux. .

O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows

Antes de instalar o pacote de plug-ins do SnapCenter para Windows, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas Operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	5 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK O Java 11 Oracle Java e OpenJDK são necessários apenas para SAP HANA, IBM Db2, PostgreSQL, MySQL, plug-ins compatíveis com NetApp e outros aplicativos personalizados que podem ser instalados no host Windows. Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux

Antes de instalar o pacote de plug-ins SnapCenter para Linux, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas operacionais	• Red Hat Enterprise Linux • Servidor SUSE Linux Enterprise (SLES) Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	2 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	Java 11 Oracle Java e OpenJDK Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em /var/opt/snapcenter/spl/etc/spl.properties esteja definida para a versão correta do JAVA e o caminho correto. Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Configurar credenciais para o plug-in SnapCenter para banco de dados SAP HANA

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter . Você deve criar credenciais para instalar plug-ins do SnapCenter e credenciais adicionais para executar operações de proteção de dados em bancos de dados ou sistemas de arquivos do Windows.

Sobre esta tarefa

- Hosts Linux

  Você deve configurar credenciais para instalar plug-ins em hosts Linux.

Você deve configurar as credenciais para o usuário root ou para um usuário não root que tenha privilégios sudo para instalar e iniciar o processo do plug-in.

Melhores práticas: embora você tenha permissão para criar credenciais para o Linux após implantar hosts e instalar plug-ins, a melhor prática é criar credenciais depois de adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

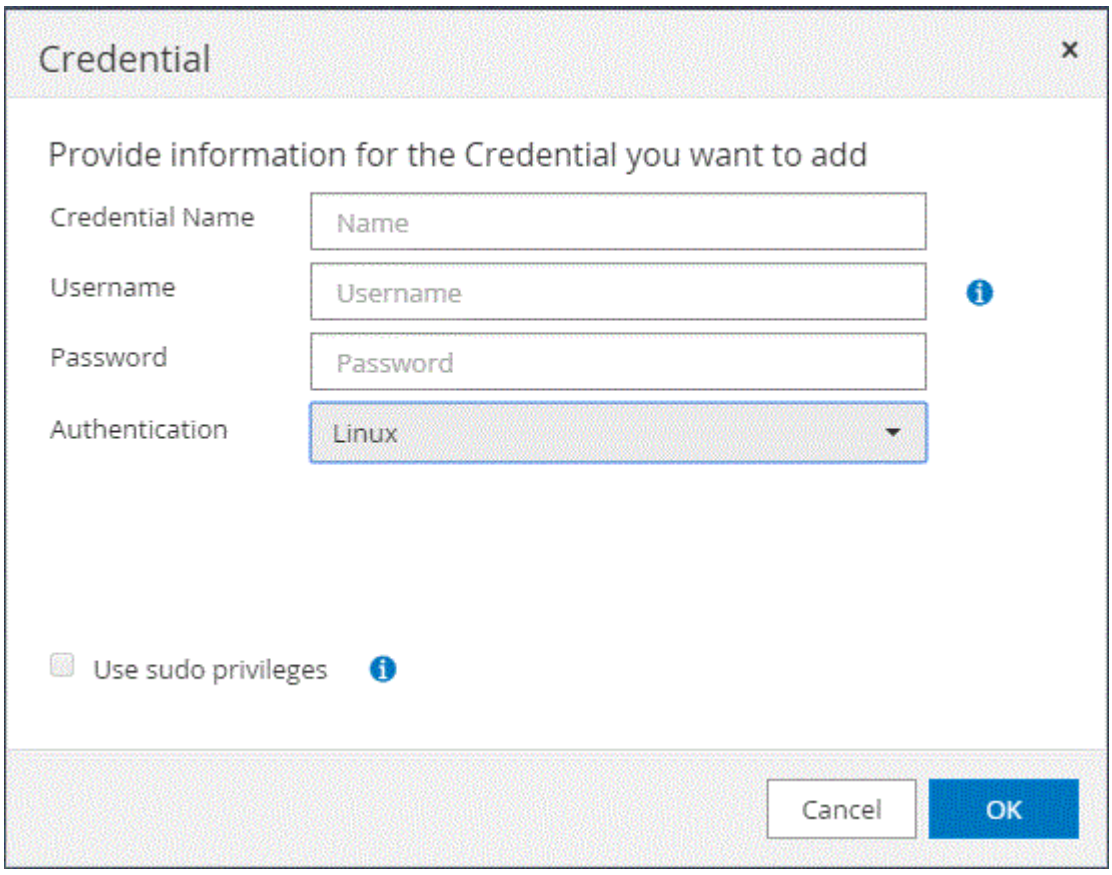
  Você deve configurar as credenciais do Windows antes de instalar plug-ins.

  Você deve configurar as credenciais com privilégios de administrador, incluindo direitos de administrador no host remoto.

Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver privilégios de administrador completos, será necessário atribuir pelo menos os privilégios de grupo de recursos e backup ao nome de usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.



4. Na página Credencial, especifique as informações necessárias para configurar as credenciais:

Para este campo…	Faça isso…
Nome da credencial	Digite um nome para as credenciais.
Nome de usuário	Digite o nome de usuário e a senha que serão usados para autenticação. • Administrador de domínio ou qualquer membro do grupo de administradores Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS\Nome do Usuário* ◦ *FQDN do domínio\Nome do usuário* • Administrador local (somente para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é: *UserName* Não use aspas duplas (") ou acento grave (`) nas senhas. Você não deve usar os símbolos de menor que (<) e exclamação (!) juntos em senhas. Por exemplo, menor que <! 10, menor que 10 <!, acento grave `12.
Senha	Digite a senha usada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que você deseja usar.
Use privilégios sudo	Marque a caixa de seleção **Usar privilégios sudo** se estiver criando credenciais para um usuário não root. Aplicável somente a usuários do Linux.

5. Clique em **OK**.

Depois de concluir a configuração das credenciais, talvez você queira atribuir a manutenção de credenciais a um usuário ou grupo de usuários na página Usuário e Acesso.

Configurar o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite que você crie uma Conta de Serviço Gerenciada de grupo (gMSA) que fornece gerenciamento automatizado de senhas de contas de serviço a partir de uma conta de domínio gerenciada.

Antes de começar

- Você deve ter um controlador de domínio do Windows Server 2016 ou posterior.
- Você deve ter um host Windows Server 2016 ou posterior, que seja membro do domínio.

Passos

1. Crie uma chave raiz do KDS para gerar senhas exclusivas para cada objeto no seu gMSA.
2. Para cada domínio, execute o seguinte comando no controlador de domínio do Windows: Add-KDSRootKey -EffectiveImmediately
3. Crie e configure seu gMSA:
   a. Crie uma conta de grupo de usuários no seguinte formato:

```
 domainName\accountName$
.. Adicione objetos de computador ao grupo.
.. Use o grupo de usuários que você acabou de criar para criar o
gMSA.
```

   Por exemplo,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correr `Get-ADServiceAccount` comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Habilite o módulo do Active Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando no PowerShell:

```
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. Reinicie seu host.

b. Instale o gMSA no seu host executando o seguinte comando no prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua privilégios administrativos ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no SnapCenter Server.

   O SnapCenter Server instalará os plug-ins selecionados no host e o gMSA especificado será usado como a conta de logon de serviço durante a instalação do plug-in.

Instalar o plug-in SnapCenter para bancos de dados SAP HANA

Adicionar hosts e instalar pacotes de plug-ins em hosts remotos

Você deve usar a página Adicionar Host do SnapCenter para adicionar hosts e, em seguida, instalar os pacotes de plug-ins. Os plug-ins são instalados automaticamente nos hosts remotos. Você pode adicionar um host e instalar pacotes de plug-in para um host individual ou para um cluster.

Antes de começar

- Se o sistema operacional do host do SnapCenter Server for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deverá executar o seguinte:
  - Atualize para o Windows Server 2019 (versão do sistema operacional 17763.5936) ou posterior
  - Atualize para o Windows Server 2022 (versão do sistema operacional 20348.2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada

ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.

- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- A documentação de administração contém informações sobre o gerenciamento de hosts.
- Se estiver usando uma conta de serviço gerenciada em grupo (gMSA), você deverá configurar a gMSA com privilégios administrativos.

  "Configurar conta de serviço gerenciada de grupo no Windows Server 2016 ou posterior para SAP HANA"

Sobre esta tarefa

- Não é possível adicionar um SnapCenter Server como um host de plug-in a outro SnapCenter Server.
- Para que a replicação do sistema SAP HANA descubra recursos nos sistemas primário e secundário, é recomendável adicionar os sistemas primário e secundário usando o usuário root ou sudo.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Clique em **Adicionar**.
4. Na página Hosts, execute as seguintes ações:

Para este campo…	Faça isso…
Tipo de host	Selecione o tipo de host: • Windows • Linux O plug-in para SAP HANA é instalado no host do cliente HDBSQL, e esse host pode estar em um sistema Windows ou Linux.
Nome do host	Digite o nome do host de comunicação. Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o FQDN. Você deve configurar o cliente HDBSQL e o HDBUserStore neste host.

Para este campo…	Faça isso…
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais. Você pode visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial fornecida. O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar Host.

5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a serem instalados.
6. (Opcional) Clique em **Mais opções**.

Para este campo…	Faça isso…
Porta	Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.
Caminho de instalação	O plug-in para SAP HANA é instalado no host do cliente HDBSQL, e esse host pode estar em um sistema Windows ou Linux. • Para o pacote de plug-ins SnapCenter para Windows, o caminho padrão é C:\Arquivos de Programas\ NetApp\ SnapCenter. Opcionalmente, você pode personalizar o caminho. • Para o pacote de plug-ins SnapCenter para Linux, o caminho padrão é /opt/ NetApp/snapcenter. Opcionalmente, você pode personalizar o caminho.

Para este campo…	Faça isso…
Ignorar verificações de pré-instalação	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.
Use a conta de serviço gerenciada em grupo (gMSA) para executar os serviços do plug-in	Para o host Windows, marque esta caixa de seleção se desejar usar a Conta de Serviço Gerenciada em Grupo (gMSA) para executar os serviços do plug-in. Forneça o nome do gMSA no seguinte formato: domainName\accountName$. O gMSA será usado como uma conta de serviço de logon somente para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

   Se você não tiver marcado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se ele atende aos requisitos para a instalação do plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão do .NET, a localização (para plug-ins do Windows) e a versão do Java (para plug-ins do Linux) são validados em relação aos requisitos mínimos. Se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas serão exibidas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em C:\Arquivos de Programas\ NetApp\ SnapCenter WebApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, deverá atualizar o arquivo em ambos os nós.

8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirmar e Enviar**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós do cluster.

   A verificação de impressão digital é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitore o progresso da instalação.

   Os arquivos de log específicos da instalação estão localizados em /custom_location/snapcenter/logs.

Instalar pacotes de plug-in SnapCenter para Linux ou Windows em vários hosts remotos usando cmdlets

Você pode instalar os pacotes de plug-in do SnapCenter para Linux ou Windows em

vários hosts simultaneamente usando o cmdlet Install-SmHostPackage do PowerShell.

Antes de começar

Você deve ter efetuado login no SnapCenter como um usuário de domínio com direitos de administrador local em cada host no qual deseja instalar o pacote de plug-in.

Passos

1. Inicie o PowerShell.
2. No host do SnapCenter Server, estabeleça uma sessão usando o cmdlet Open-SmConnection e insira suas credenciais.
3. Instale o plug-in em vários hosts usando o cmdlet Install-SmHostPackage e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

   Você pode usar a opção -skipprecheck quando tiver instalado os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

4. Insira suas credenciais para instalação remota.

Instale o plug-in SnapCenter para banco de dados SAP HANA em hosts Linux usando a interface de linha de comando

Você deve instalar o SnapCenter Plug-in para o banco de dados SAP HANA usando a interface de usuário (IU) do SnapCenter . Se o seu ambiente não permitir a instalação remota do plug-in pela interface do usuário do SnapCenter , você poderá instalar o plug-in para o banco de dados SAP HANA no modo de console ou no modo silencioso usando a interface de linha de comando (CLI).

Antes de começar

- Você deve instalar o plug-in para o banco de dados SAP HANA em cada host Linux onde o cliente HDBSQL reside.
- O host Linux no qual você está instalando o SnapCenter Plug-in para o banco de dados SAP HANA deve atender aos requisitos de software, banco de dados e sistema operacional dependentes.

  A Ferramenta de Matriz de Interoperabilidade (IMT) contém as informações mais recentes sobre as configurações suportadas.

  https://imt.netapp.com/matrix/imt.jsp?components=121029;&solution=1259&isHWU&src=IMT

- O plug-in SnapCenter para banco de dados SAP HANA faz parte do pacote de plug-ins SnapCenter para Linux. Antes de instalar o SnapCenter Plug-ins Package para Linux, você já deve ter instalado o SnapCenter em um host Windows.

Passos

1. Copie o arquivo de instalação do pacote de plug-ins SnapCenter para Linux (snapcenter_linux_host_plugin.bin) de C:\ProgramData\ NetApp\ SnapCenter\Package Repository para o host onde você deseja instalar o plug-in para o banco de dados SAP HANA.

   Você pode acessar esse caminho a partir do host onde o SnapCenter Server está instalado.

2. No prompt de comando, navegue até o diretório onde você copiou o arquivo de instalação.
3. Instale o plug-in: `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 especifica a porta de comunicação HTTPS do SMCore.
   - -DSERVER_IP especifica o endereço IP do SnapCenter Server.
   - -DSERVER_HTTPS_PORT especifica a porta HTTPS do SnapCenter Server.
   - -DUSER_INSTALL_DIR especifica o diretório onde você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
   - DINSTALL_LOG_NAME especifica o nome do arquivo de log.

```
/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. Edite o arquivo /<diretório de instalação>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties e adicione o parâmetro PLUGINS_ENABLED = hana:3.0.
5. Adicione o host ao SnapCenter Server usando o cmdlet Add-Smhost e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitore o status da instalação do Plug-in para SAP HANA

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.

3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
   a. Clique em **Filtrar**.
   b. Opcional: especifique a data de início e término.
   c. No menu suspenso Tipo, selecione **Instalação de plug-in**.
   d. No menu suspenso Status, selecione o status da instalação.
   e. Clique em **Aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Configurar certificado CA

Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.

O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte "Como gerar um arquivo CSR de certificado CA" .

Se você possui o certificado CA para seu domínio (*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.

5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Importar chave privada	Selecione a opção **Sim**, importe a chave privada e clique em **Avançar**.
Formato de arquivo de importação	Não faça alterações; clique em **Avançar**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

> O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: *.pfx, *.p12 e *.p7b).

7. Repita a Etapa 5 para a pasta “Pessoal”.

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

Passos

1. Execute o seguinte na GUI:
   a. Clique duas vezes no certificado.
   b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.
   c. Percorra a lista de campos e clique em **Impressão digital**.
   d. Copie os caracteres hexadecimais da caixa.
   e. Remova os espaços entre os números hexadecimais.

      Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
   a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copie a impressão digital.

Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Por exemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Vincule o certificado recém-instalado aos serviços de plug-in do host
   do Windows, executando os seguintes comandos:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Por exemplo:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

Configurar o certificado CA para o serviço SnapCenter SAP HANA Plug-ins no host Linux

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo 'keystore.jks', que está localizado em */opt/ NetApp/snapcenter/scc/etc* como seu armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in a partir do arquivo de propriedades do agente do plug-in.

   É o valor correspondente à chave 'KEYSTORE_PASS'.

2. Alterar a senha do keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Altere a senha de todos os aliases de entradas de chave privada no
keystore para a mesma senha usada para o keystore:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

   Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

3. Reinicie o serviço após alterar a senha.

> A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Reinicie o serviço após configurar os certificados raiz ou
intermediários para conectar o trust-store.
```

> Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Adicione o certificado da CA com chave privada e pública.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Listar os certificados adicionados no keystore.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

   A senha padrão do keystore do plug-in é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Se o nome do alias no certificado da CA for longo e contiver espaços
   ou caracteres especiais ("*",","), altere o nome do alias para um nome
   simples:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configure o nome do alias do certificado CA no arquivo
   agent.properties.
   ```

   Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

Configurar lista de revogação de certificados (CRL) para plug-ins

Sobre esta tarefa

- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é ' opt/ NetApp/snapcenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties em relação à chave CRL_PATH.

   Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados

em relação a cada CRL.

Configurar o certificado CA para o serviço SnapCenter SAP HANA Plug-ins no host Windows

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo *keystore.jks*, que está localizado em *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* como seu armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in a partir do arquivo de propriedades do agente do plug-in.

   É o valor correspondente à chave *KEYSTORE_PASS*.

2. Alterar a senha do keystore:

   keytool -storepasswd -keystore keystore.jks

   > Se o comando "keytool" não for reconhecido no prompt de comando do Windows, substitua o comando keytool pelo seu caminho completo.

   C:\Arquivos de Programas\Java\<versão_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. Altere a senha de todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:

   keytool -keypasswd -alias "nome_do_alias_no_certificado" -keystore keystore.jks

   Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

4. Reinicie o serviço após alterar a senha.

   > A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

keytool -list -v -keystore keystore.jks

4. Adicione um certificado raiz ou intermediário:

   keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Reinicie o serviço após configurar os certificados raiz ou intermediários para conectar o trust-store.

   Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo *keystore.jks*.
3. Listar os certificados adicionados no keystore:

   keytool -list -v -keystore keystore.jks

4. Adicione o certificado da CA com chave privada e pública.

   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS

5. Listar os certificados adicionados no keystore.

   keytool -list -v -keystore keystore.jks

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

   A senha padrão do keystore do plug-in é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

   keytool -keypasswd -alias "nome_do_alias_no_certificado_da_CA" -keystore keystore.jks

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

   Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

Configurar lista de revogação de certificados (CRL) para plug-ins SnapCenter

Sobre esta tarefa

- Para baixar o arquivo CRL mais recente para o certificado CA relacionado, consulte "Como atualizar o arquivo de lista de revogação de certificados no SnapCenter CA Certificate" .
- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é *'C:\Arquivos de Programas*\

NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo *agent.properties* em relação à chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

   Os certificados recebidos serão verificados em relação a cada CRL.

Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *Get-SmCertificateSettings*.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- *  * indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- *  * indica que o certificado CA foi validado com sucesso.
- *  * indica que o certificado CA não pôde ser validado.
- * * indica que as informações de conexão não puderam ser recuperadas.

Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Instalar o SnapCenter Plug-in for VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs), ou se você quiser proteger VMs e armazenamentos de dados, será

necessário implantar o SnapCenter Plug-in for VMware vSphere .

Para obter informações sobre como implantar, consulte "Visão geral da implantação" .

Implantar certificado CA

Para configurar o Certificado CA com o SnapCenter Plug-in for VMware vSphere, consulte "Criar ou importar certificado SSL" .

Configurar o arquivo CRL

O SnapCenter Plug-in for VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL do SnapCenter Plug-in for VMware vSphere é */opt/netapp/config/crl*.

Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Prepare-se para a proteção de dados

Pré-requisitos para usar o plug-in SnapCenter para banco de dados SAP HANA

Antes de usar o SnapCenter Plug-in para o banco de dados SAP HANA, o administrador do SnapCenter deve instalar e configurar o SnapCenter Server e executar as tarefas de pré-requisito.

- Instalar e configurar o SnapCenter Server.
- Efetue login no SnapCenter Server.
- Configure o ambiente SnapCenter adicionando conexões do sistema de armazenamento e criando credenciais, se aplicável.
- Instale o Java 11 no seu host Linux ou Windows.

  Você deve definir o caminho Java na variável de caminho ambiental da máquina host.

- Configure o SnapMirror e o SnapVault se desejar replicação de backup.
- Instale o cliente HDBSQL no host onde você instalará o plug-in para o banco de dados SAP HANA.

  Configure as chaves de armazenamento do usuário para os nós do SAP HANA que você gerenciará por meio deste host.

- Para o banco de dados SAP HANA 2.0SPS05, se você estiver usando uma conta de usuário do banco de dados SAP HANA, certifique-se de ter as seguintes permissões para executar operações de backup, restauração e clonagem no SnapCenter Server:
  - Administrador de backup
  - Leitura do catálogo
  - Administrador de backup de banco de dados
  - Operador de recuperação de banco de dados

Como recursos, grupos de recursos e políticas são usados para proteger bancos de dados SAP HANA

Antes de usar o SnapCenter, é útil entender os conceitos básicos relacionados às operações de backup, clonagem e restauração que você deseja executar. Você interage com recursos, grupos de recursos e políticas para diferentes operações.

- Os recursos geralmente são bancos de dados SAP HANA que você faz backup ou clona com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host.

  Ao executar uma operação em um grupo de recursos, você executa essa operação nos recursos definidos no grupo de recursos de acordo com o cronograma especificado para o grupo de recursos.

  Você pode fazer backup sob demanda de um único recurso ou de um grupo de recursos. Você também pode executar backups agendados para recursos individuais e grupos de recursos.

- As políticas especificam a frequência de backup, replicação, scripts e outras características das operações de proteção de dados.

  Ao criar um grupo de recursos, você seleciona uma ou mais políticas para esse grupo. Você também pode selecionar uma política ao executar um backup sob demanda para um único recurso.

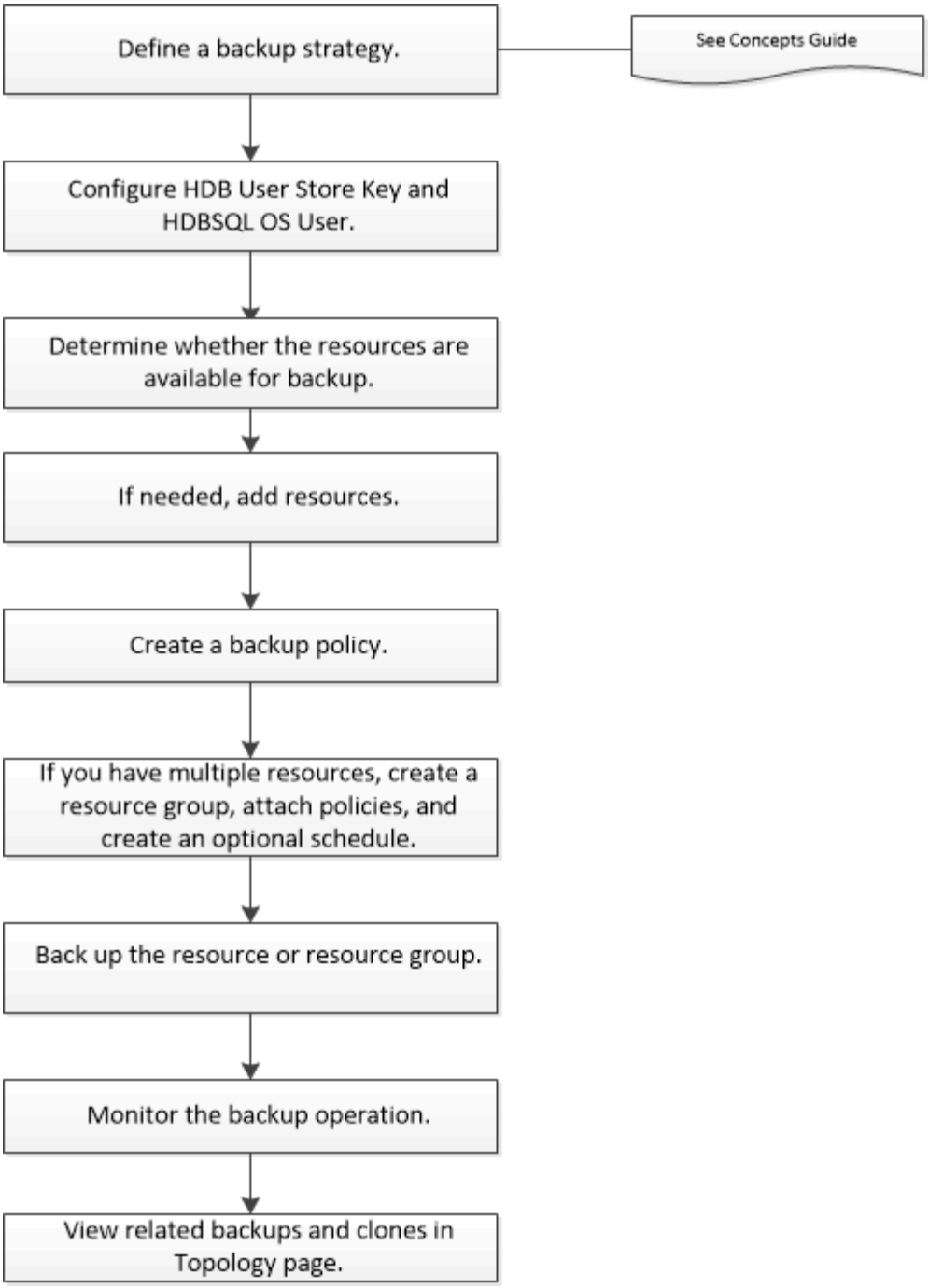
Pense em um grupo de recursos como algo que define o que você quer proteger e quando quer proteger em termos de dia e hora. Pense em uma política como a definição de como você deseja protegê-la. Se você estiver fazendo backup de todos os bancos de dados, por exemplo, poderá criar um grupo de recursos que inclua todos os bancos de dados no host. Você pode então anexar duas políticas ao grupo de recursos: uma política diária e uma política horária. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diariamente.

Fazer backup dos recursos do SAP HANA

Fazer backup dos recursos do SAP HANA

Você pode criar um backup de um recurso (banco de dados) ou grupo de recursos. O fluxo de trabalho de backup inclui planejamento, identificação dos bancos de dados para backup, gerenciamento de políticas de backup, criação de grupos de recursos e anexação de políticas, criação de backups e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de backup:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell. "Guia de referência do cmdlet do software SnapCenter" .

Configurar a chave de armazenamento do usuário HDB e o usuário do sistema operacional HDBSQL para o banco de dados SAP HANA

Você deve configurar a chave de armazenamento do usuário HDB e o usuário do sistema operacional HDBSQL para executar operações de proteção de dados em bancos de dados SAP HANA.

Antes de começar

- Se o banco de dados SAP HANA não tiver a chave de armazenamento de usuário seguro do HDB e o usuário do sistema operacional SQL do HDB configurados, um ícone de cadeado vermelho aparecerá somente para os recursos descobertos automaticamente. Se, durante uma operação de descoberta subsequente, a chave de armazenamento de usuário segura do HDB configurada for considerada incorreta ou não fornecer acesso ao próprio banco de dados, o ícone de cadeado vermelho reaparecerá.
- Você deve configurar a chave de armazenamento de usuário seguro do HDB e o usuário do sistema operacional SQL do HDB para poder proteger o banco de dados ou adicioná-lo a um grupo de recursos para executar operações de proteção de dados.
- Você deve configurar o usuário do sistema operacional HDB SQL para acessar o banco de dados do sistema. Se o usuário do sistema operacional HDB SQL estiver configurado para acessar somente o banco de dados do locatário, a operação de descoberta falhará.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione Plug-in SnapCenter para banco de dados SAP HANA na lista.
2. Na página Recursos, selecione o tipo de recurso na lista **Exibir**.
3. (Opcional) Clique e selecione o nome do host.

   Você pode então clicar para fechar o painel de filtro.
4. Selecione o banco de dados e clique em **Configurar banco de dados**.
5. Na seção Configurar definições do banco de dados, insira a Chave de armazenamento de usuário seguro do HDB.

   O nome do host do plug-in é exibido e o usuário do sistema operacional HDB SQL é preenchido automaticamente como <sid>adm.
6. Clique em **OK**.

Você pode modificar a configuração do banco de dados na página Topologia.

Descubra recursos e prepare contêineres de banco de dados multilocatários para proteção de dados

Descubra os bancos de dados automaticamente

Os recursos são bancos de dados SAP HANA e volumes não relacionados a dados no host Linux que são gerenciados pelo SnapCenter. Você pode adicionar esses recursos a grupos de recursos para executar operações de proteção de dados depois de descobrir os bancos de dados SAP HANA que estão disponíveis.

Antes de começar

- Você já deve ter concluído tarefas como instalar o SnapCenter Server, adicionar a chave de armazenamento do usuário do HDB, adicionar hosts e configurar as conexões do sistema de armazenamento.
- Você deve ter configurado a chave de armazenamento de usuário seguro do HDB e o usuário do sistema operacional SQL do HDB no host Linux.
  - Você deve configurar a chave de armazenamento do usuário HDB com o SID adm user. Por exemplo, para o sistema HANA com A22 como SID, a chave de armazenamento do usuário HDB deve ser

configurada com a22adm.

- O plug-in SnapCenter para banco de dados SAP HANA não oferece suporte à descoberta automática de recursos que residem em ambientes virtuais RDM/VMDK. Você deve fornecer as informações de armazenamento para ambientes virtuais ao adicionar os bancos de dados manualmente.

Sobre esta tarefa

Após instalar o plug-in, todos os recursos naquele host Linux são descobertos automaticamente e exibidos na página Recursos.

Os recursos descobertos automaticamente não podem ser modificados ou excluídos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o Plug-in para Banco de Dados SAP HANA na lista.
2. Na página Recursos, selecione o tipo de recurso na lista Exibir.
3. (Opcional) Clique em * * e, em seguida, selecione o nome do host.

   Você pode então clicar em * * para fechar o painel de filtro.

4. Clique em **Atualizar recursos** para descobrir os recursos disponíveis no host.

   Os recursos são exibidos junto com informações como tipo de recurso, nome do host, grupos de recursos associados, tipo de backup, políticas e status geral.

   - Se o banco de dados estiver em um armazenamento NetApp e não estiver protegido, Não protegido será exibido na coluna Status geral.
   - Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, e se nenhuma operação de backup for realizada, Backup não executado será exibido na coluna Status geral. Caso contrário, o status mudará para Falha no backup ou Backup bem-sucedido com base no último status do backup.

Se o banco de dados SAP HANA não tiver uma chave de armazenamento de usuário segura HDB configurada, um ícone de cadeado vermelho aparecerá ao lado do recurso. Se, durante uma operação de descoberta subsequente, a chave de armazenamento de usuário segura do HDB configurada for considerada incorreta ou não fornecer acesso ao próprio banco de dados, o ícone de cadeado vermelho reaparecerá.

Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

Depois que você terminar

Você deve configurar a chave de armazenamento do usuário seguro do HDB e o usuário do sistema operacional HDBSQL para poder proteger o banco de dados ou adicioná-lo ao grupo de recursos para executar operações de proteção de dados.

"Configurar a chave de armazenamento do usuário HDB e o usuário do sistema operacional HDBSQL para o banco de dados SAP HANA"

Preparar contêineres de banco de dados multilocatário para proteção de dados

Para hosts SAP HANA registrados diretamente no SnapCenter, a instalação ou atualização do SnapCenter Plug-in para banco de dados SAP HANA acionará uma

descoberta automática de recursos no host. Após instalar ou atualizar o plug-in, para cada recurso de contêiner de banco de dados multilocatário (MDC) localizado no host do plug-in, outro recurso MDC será descoberto automaticamente com um formato GUID diferente e registrado no SnapCenter. O novo recurso estará no estado “bloqueado”.

Sobre esta tarefa

Por exemplo, no SnapCenter 4.2, se o recurso E90 MDC estava localizado no host do plug-in e registrado manualmente, após a atualização para o SnapCenter 4.3, outro recurso E90 MDC com um GUID diferente será descoberto e registrado no SnapCenter.

> Os backups associados ao recurso do SnapCenter 4.2 e versões anteriores devem ser mantidos até o término do período de retenção. Após o término do período de retenção, você pode excluir o antigo recurso MDC e continuar a gerenciar o novo recurso MDC descoberto automaticamente.

`Old MDC resource`é o recurso MDC para um host de plug-in que foi adicionado manualmente no SnapCenter 4.2 ou versões anteriores.

Execute as seguintes etapas para começar a usar o novo recurso descoberto no SnapCenter 4.3 para operações de proteção de dados:

Passos

1. Na página Recursos, selecione o antigo recurso MDC com backups adicionados à versão anterior do SnapCenter e coloque-o no “modo de manutenção” na página Topologia.

   Se o recurso fizer parte de um grupo de recursos, coloque o grupo de recursos no “modo de manutenção”.

2. Configure o novo recurso MDC descoberto após a atualização para o SnapCenter 4.3 selecionando o novo recurso na página Recursos.

   “Novo recurso MDC” é o recurso MDC recém-descoberto que foi descoberto quando o SnapCenter Server e o host do plug-in foram atualizados para 4.3. O novo recurso MDC pode ser identificado como um recurso com o mesmo SID que o antigo recurso MDC, para um determinado host, e com um ícone de cadeado vermelho ao lado dele na página Recursos.

3. Proteja o novo recurso MDC descoberto após a atualização para o SnapCenter 4.3 selecionando políticas de proteção, agendamentos e configurações de notificação.
4. Exclua os backups feitos no SnapCenter 4.2 ou versões anteriores com base nas configurações de retenção.
5. Exclua o grupo de recursos da página Topologia.
6. Exclua o antigo recurso MDC da página Recursos.

   Por exemplo, se o período de retenção de Snapshots primários for de 7 dias e o período de retenção de Snapshots secundários for de 45 dias, após a conclusão dos 45 dias e após a exclusão de todos os backups, você deverá excluir o grupo de recursos e o antigo recurso MDC.

Informações relacionadas

"Configurar a chave de armazenamento do usuário HDB e o usuário do sistema operacional HDBSQL para o banco de dados SAP HANA"

"Visualize backups e clones do banco de dados SAP HANA na página Topologia"

Adicionar recursos manualmente ao host do plug-in

A descoberta automática não é suportada para determinadas instâncias do HANA. Você deve adicionar esses recursos manualmente.

Antes de começar

- Você deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts, configurar conexões do sistema de armazenamento e adicionar a chave de armazenamento do usuário do HDB.
- Para replicação do sistema SAP HANA, é recomendável adicionar todos os recursos desse sistema HANA em um grupo de recursos e fazer um backup do grupo de recursos. Isso garante um backup perfeito durante o modo de failback de aquisição.

"Crie grupos de recursos e anexe políticas" .

Sobre esta tarefa

A descoberta automática não é suportada para as seguintes configurações:

- Layouts RDM e VMDK

> Caso os recursos acima sejam descobertos, as operações de proteção de dados não serão suportadas nesses recursos.

- Configuração de múltiplos hosts do HANA
- Várias instâncias no mesmo host
- Replicação do sistema HANA com escalonamento multicamadas
- Ambiente de replicação em cascata no modo de replicação do sistema

Passos

1. No painel de navegação esquerdo, selecione o plug-in SnapCenter para banco de dados SAP HANA na lista suspensa e clique em **Recursos**.
2. Na página Recursos, clique em **Adicionar banco de dados SAP HANA**.
3. Na página Fornecer detalhes do recurso, execute as seguintes ações:

Para este campo…	Faça isso…
Tipo de recurso	Insira o tipo de recurso. Os tipos de recursos são Contêiner Único, Contêiner de Banco de Dados Multilocatário (MDC) e Volume sem dados.
Nome do sistema HANA	Insira o nome descritivo do sistema SAP HANA. Esta opção só estará disponível se você selecionar os tipos de recursos Contêiner Único ou MDC.
SID	Digite o ID do sistema (SID). O sistema SAP HANA instalado é identificado por um único SID.
Host de plug-in	Selecione o host do plug-in.

Para este campo…	Faça isso…
Chaves de armazenamento de usuário seguro HDB	Insira a chave para conectar ao sistema SAP HANA. A chave contém as informações de login para conectar ao banco de dados. Para a replicação do sistema SAP HANA, a chave de usuário secundária não é validada. Isso será usado durante a aquisição.
Usuário do sistema operacional HDBSQL	Digite o nome de usuário para o qual a chave de armazenamento de usuário seguro do HDB está configurada. No Windows, é obrigatório que o usuário do sistema operacional HDBSQL seja o usuário SYSTEM. Portanto, você deve configurar a chave de armazenamento do usuário seguro do HDB para o usuário SYSTEM.

4. Na página Fornecer espaço de armazenamento, selecione um sistema de armazenamento e escolha um ou mais volumes, LUNs e qtrees e clique em **Salvar**.

   Opcional: Você pode clicar no * * ícone para adicionar mais volumes, LUNs e qtrees de outros sistemas de armazenamento.

5. Revise o resumo e clique em **Concluir**.

   Os bancos de dados são exibidos junto com informações como SID, host do plug-in, grupos de recursos e políticas associados e status geral

Se você quiser fornecer aos usuários acesso aos recursos, deverá atribuir os recursos aos usuários. Isso permite que os usuários executem as ações para as quais têm permissão nos ativos atribuídos a eles.

"Adicionar um usuário ou grupo e atribuir função e ativos"

Depois de adicionar os bancos de dados, você pode modificar os detalhes do banco de dados SAP HANA.

Não será possível modificar o seguinte se houver backups associados ao recurso SAP HANA:

- Contêineres de banco de dados multilocatário (MDC): SID ou Host do cliente HDBSQL (plug-in)
- Contêiner único: SID ou host do cliente HDBSQL (plug-in)
- Volume não relacionado a dados: nome do recurso, SID associado ou host do plug-in

Crie políticas de backup para bancos de dados SAP HANA

Antes de usar o SnapCenter para fazer backup de recursos do banco de dados SAP HANA, você deve criar uma política de backup para o recurso ou grupo de recursos que deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e mantém backups.

Antes de começar

- Você deve ter definido sua estratégia de backup.

  Para obter detalhes, consulte as informações sobre como definir uma estratégia de proteção de dados para bancos de dados SAP HANA.

- Você deve ter se preparado para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, configurar conexões do sistema de armazenamento e adicionar recursos.
- O administrador do SnapCenter deve ter atribuído as SVMs para os volumes de origem e destino a você se estiver replicando Snapshots para um espelho ou cofre.

  Além disso, você pode especificar configurações de replicação, script e aplicativo na política. Essas opções economizam tempo quando você deseja reutilizar a política para outro grupo de recursos.

- Revise os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror . Para obter informações, consulte "Limites de objetos para sincronização ativa do SnapMirror" .

Sobre esta tarefa

- Replicação do sistema SAP HANA
  - Você pode proteger o sistema SAP HANA primário e todas as operações de proteção de dados podem ser executadas.
  - Você pode proteger o sistema SAP HANA secundário, mas os backups não podem ser criados.

    Após o failover, todas as operações de proteção de dados podem ser executadas, pois o sistema SAP HANA secundário se torna o sistema SAP HANA primário.

  Não é possível criar um backup para o volume de dados do SAP HANA, mas o SnapCenter continua protegendo os volumes não relacionados a dados (NDV).

- SnapLock
  - Se a opção 'Manter as cópias de backup por um número específico de dias' for selecionada, o período de retenção do SnapLock deverá ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio de Snapshot impede a exclusão dos Snapshots até que o período de retenção expire. Isso pode levar à retenção de um número maior de Snapshots do que a contagem especificada na política.
  - Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Clique em **Novo**.
4. Na página Nome, insira o nome e os detalhes da política.
5. Na página Tipo de política, execute as seguintes etapas:
   - Escolha o tipo de armazenamento
   - Escolha o tipo de backup:

Se você quiser…	Faça isso…
Crie um backup usando a tecnologia Snapshot	Selecione **Baseado em instantâneo**.
Executar uma verificação de integridade do banco de dados	Selecione **Backup baseado em arquivo**. Somente locatários ativos são copiados.

6. Na página Snapshot e Replicação, execute as seguintes etapas:
   - Especifique o tipo de programação selecionando **Sob demanda**, **Por hora**, **Diário**, **Semanal** ou **Mensal**.

> Você pode especificar o agendamento (data de início, data de término e frequência) para a operação de backup ao criar um grupo de recursos. Isso permite que você crie grupos de recursos que compartilham a mesma política e frequência de backup, mas também permite que você atribua diferentes agendamentos de backup a cada política.

> Se você agendou para 2h00, a programação não será acionada durante o horário de verão (DST).

7. Na página Snapshot e Replicação, especifique as configurações de retenção para o tipo de backup e o tipo de agendamento selecionado na página Tipo de backup:

Se você quiser…	Então…
Mantenha um certo número de Snapshots	Selecione **Cópias a serem mantidas** e especifique o número de Snapshots que você deseja manter. Se o número de Snapshots exceder o número especificado, os Snapshots mais antigos serão excluídos primeiro. O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida como um valor maior do que o suportado pela versão do ONTAP . Para backups baseados em cópia de instantâneo, você deve definir a contagem de retenção como 2 ou mais se planeja habilitar a replicação do SnapVault . Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro Snapshot será o Snapshot de referência para o relacionamento SnapVault até que um Snapshot mais recente seja replicado para o destino. Para replicação do sistema SAP HANA, é recomendável adicionar todos os recursos do sistema SAP HANA em um grupo de recursos. Isso garante que o número correto de backups seja mantido. Para a replicação do sistema SAP HANA, o total de snapshots obtidos será igual ao conjunto de retenção para o grupo de recursos. A remoção do Snapshot mais antigo é baseada em qual nó o Snapshot mais antigo está localizado. Por exemplo, a retenção é definida como 7 para um grupo de recursos com SAP HANA System Replication primário e SAP HANA System Replication secundário. Você pode tirar no máximo 7 snapshots por vez, incluindo o SAP HANA System Replication primário e o SAP HANA System Replication secundário.

Se você quiser…	Então…
Mantenha os Snapshots por um certo número de dias	Selecione **Manter cópias por** e especifique o número de dias pelos quais você deseja manter os Snapshots antes de excluí-los.
Período de bloqueio de cópia de instantâneo	Selecione **Período de bloqueio de cópia de instantâneo** e especifique dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

8. Selecione um rótulo de Snapshot.

> Você pode atribuir rótulos SnapMirror a snapshots primários para replicação remota, permitindo que os snapshots primários descarreguem a operação de replicação de snapshots do SnapCenter para sistemas secundários ONTAP . Isso pode ser feito sem habilitar a opção SnapMirror ou SnapVault na página de política.

9. Para backups baseados em cópia de instantâneo, na seção Selecionar opções de replicação secundária, selecione uma ou ambas as seguintes opções de replicação secundária:

Para este campo…	Faça isso…
Atualize o SnapMirror após criar uma cópia local do Snapshot	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Esta opção deve ser habilitada para sincronização ativa do SnapMirror . Se o relacionamento de proteção no ONTAP for do tipo Espelho e Cofre e se você selecionar apenas esta opção, o Snapshot criado no primário não será transferido para o destino, mas será listado no destino. Se este Snapshot for selecionado no destino para executar uma operação de restauração, a mensagem de erro O local secundário não estará disponível para o backup em cofre/espelhado selecionado será exibida. Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Ver "Visualize backups e clones do banco de dados SAP HANA na página Topologia" .

Para este campo…	Faça isso…
Atualize o SnapVault após criar uma cópia local do Snapshot	Selecione esta opção para executar a replicação de backup de disco para disco (backups do SnapVault). Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Quando o SnapLock é configurado somente no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página Topologia atualiza o período de bloqueio no secundário recuperado do ONTAP. Para mais informações sobre o SnapLock Vault, consulte "Enviar cópias do Snapshot para o WORM em um destino de cofre" Ver "Visualize backups e clones do banco de dados SAP HANA na página Topologia" .
Erro na contagem de novas tentativas	Insira o número máximo de tentativas de replicação que podem ser permitidas antes que a operação seja interrompida.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o armazenamento secundário para evitar atingir o limite máximo de Snapshots no armazenamento secundário.

10. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas

Um grupo de recursos é o contêiner ao qual você deve adicionar recursos que deseja fazer backup e proteger. Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente. Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que deseja executar.

Sobre esta tarefa

- Para criar backups de replicação do sistema SAP HANA, é recomendável adicionar todos os recursos do sistema SAP HANA em um grupo de recursos. Isso garante um backup perfeito durante o modo de failback de aquisição.
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots

como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

- Não há suporte para adicionar novos bancos de dados sem sincronização ativa do SnapMirror a um grupo de recursos existente que contém recursos com sincronização ativa do SnapMirror .
- Não há suporte para adicionar novos bancos de dados a um grupo de recursos existente no modo de failover da sincronização ativa do SnapMirror . Você pode adicionar recursos ao grupo de recursos somente no estado regular ou de failback.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Insira um nome para o grupo de recursos. O nome do grupo de recursos não deve exceder 250 caracteres.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.
Use formato de nome personalizado para cópia do Snapshot	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot. Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

4. Na página Recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Tipo de recurso**.

   Isso ajuda a filtrar informações na tela.

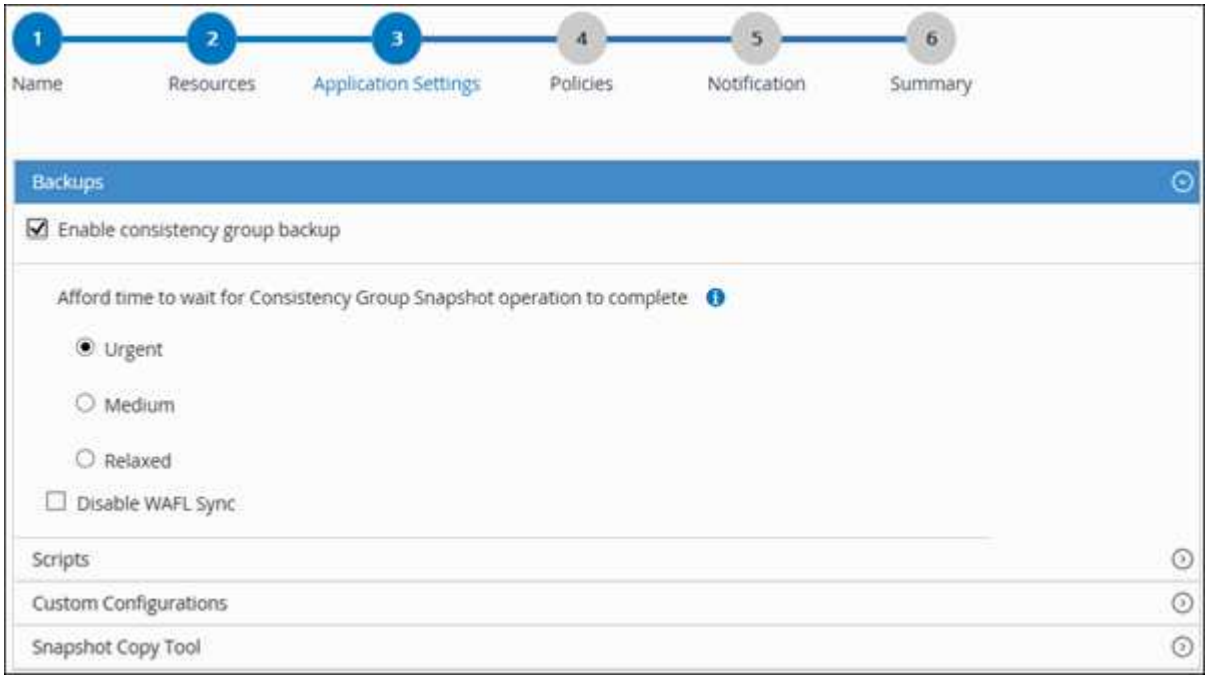
5. Selecione os recursos na seção **Recursos disponíveis** e clique na seta para a direita para movê-los para a seção **Recursos selecionados**.
6. Na página Configurações do aplicativo, faça o seguinte:

   a. Clique na seta **Backups** para definir opções adicionais de backup:

      Habilite o backup do grupo de consistência e execute as seguintes tarefas:

Para este campo…	Faça isso…
Permitir tempo de espera para que a operação do Consistency Group Snapshot seja concluída	Selecione **Urgente**, **Médio** ou **Relaxado** para especificar o tempo de espera para a conclusão da operação de Snapshot. Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.
Desativar sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL .

+



a. Clique na seta **Scripts** e insira os comandos pre e post para operações de inatividade, Snapshot e unquiesce. Você também pode inserir os pré-comandos a serem executados antes de sair em caso de falha.

b. Clique na seta **Configurações personalizadas** e insira os pares de chave-valor personalizados necessários para todas as operações de proteção de dados que usam este recurso.

Parâmetro	Contexto	Descrição
HABILITAR_REGISTRO_DE_ARQUIVO	(S/N)	Permite que o gerenciamento de log de arquivamento exclua os logs de arquivamento.

Parâmetro	Contexto	Descrição
RETENÇÃO_DE_REGISTRO_DE_ARQUIVO	número_de_dias	Especifica o número de dias que os logs de arquivamento são retidos. Esta configuração deve ser igual ou maior que NTAP_SNAPSHOT_ RETENTIONS.
DIRETÓRIO_DE_LOG_DE_ARQUIVO	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs de arquivamento.
EXT_DE_LOG_DE_ARQUIVO	extensão_de_arquivo	Especifica o comprimento da extensão do arquivo de log de arquivamento. Por exemplo, se o log de arquivamento for log_backup_0_0_0_0.16151855 1942 9 e se o valor file_extension for 5, a extensão do log manterá 5 dígitos, que é 16151.
ARQUIVO_LOG_RECURSIVO_SE ARQUIVO	(S/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs de arquivamento estiverem localizados em subdiretórios.

Os pares de chave-valor personalizados são suportados para sistemas de plug-in SAP HANA Linux e não são suportados para o banco de dados SAP HANA registrado como um plug-in centralizado do Windows.

c. Clique na seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar Instantâneos:

Se você quiser…	Então…
SnapCenter para usar o plug-in para Windows e colocar o sistema de arquivos em um estado consistente antes de criar um Snapshot. Para recursos do Linux, esta opção não é aplicável.	Selecione * SnapCenter com consistência do sistema de arquivos*. Esta opção não é aplicável ao SnapCenter Plug-in para banco de dados SAP HANA.

Se você quiser…	Então…
SnapCenter para criar um instantâneo de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.
Para inserir o comando a ser executado no host para criar cópias de Snapshot.	Selecione **Outro** e insira o comando a ser executado no host para criar um Snapshot.

7. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em * + *.

      As políticas são listadas na seção Configurar agendamentos para políticas selecionadas.

   b. Na coluna Configurar agendamentos, clique em * + * para a política que você deseja configurar.

   c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

      Onde policy_name é o nome da política que você selecionou.

      Os agendamentos configurados são listados na coluna **Agendamentos Aplicados**.

   Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. O servidor SMTP deve ser configurado em **Configurações** > **Configurações globais**.

9. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e habilite proteção secundária para recursos SAP HANA em sistemas ASA r2

Você deve criar o grupo de recursos para adicionar os recursos que estão nos sistemas ASA r2. Você também pode provisionar a proteção secundária ao criar o grupo de recursos.

Antes de começar

- Você deve garantir que não está adicionando recursos do ONTAP 9.x e recursos do ASA r2 ao mesmo grupo de recursos.
- Você deve garantir que não tenha um banco de dados com recursos ONTAP 9.x e recursos ASA r2.

Sobre esta tarefa

- A proteção secundária estará disponível somente se o usuário conectado estiver atribuído à função que

tem o recurso **SecondaryProtection** habilitado.

- Se você habilitar a proteção secundária, o grupo de recursos será colocado no modo de manutenção durante a criação dos grupos de consistência primário e secundário. Depois que os grupos de consistência primário e secundário são criados, o grupo de recursos é retirado do modo de manutenção.
- O SnapCenter não oferece suporte à proteção secundária para um recurso clone.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:
   a. Insira um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 caracteres.

   b. Insira um ou mais rótulos no campo Tag para ajudar você a pesquisar o grupo de recursos posteriormente.

      Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.

   c. Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

      Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

   d. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

      Você deve usar exatamente o mesmo destino definido no aplicativo, incluindo o prefixo, se necessário.

4. Na página Recursos, selecione o nome do host do banco de dados na lista suspensa **Host**.

   Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos do ASA r2 na seção Recursos disponíveis e mova-os para a seção Recursos selecionados.
6. Na página Configurações do aplicativo, selecione a opção de backup.
7. Na página Políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em + .

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

Onde *policy_name* é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Se a proteção secundária estiver habilitada para a política selecionada, a página Proteção Secundária será exibida e você precisará executar as seguintes etapas:

a. Selecione o tipo de política de replicação.

A política de replicação síncrona não é suportada.

b. Especifique o sufixo do grupo de consistência que você deseja usar.

c. Nos menus suspensos Cluster de destino e SVM de destino, selecione o cluster emparelhado e o SVM que você deseja usar.

O cluster e o peering de SVM não são suportados pelo SnapCenter. Você deve usar o System Manager ou as CLIs do ONTAP para executar o peering de cluster e SVM.

Se os recursos já estiverem protegidos fora do SnapCenter, eles serão exibidos na seção Recursos Protegidos Secundários.

1. Na página Verificação, execute as seguintes etapas:

a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para realizar a verificação no armazenamento secundário.

b. Clique + na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política.

c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name, execute as seguintes ações:

Se você quiser…	**Faça isso…**
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

d. Selecione **Verificar no local secundário** para verificar seus backups no sistema de armazenamento secundário.

e. Clique em **OK**.

Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

2. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

   Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

3. Revise o resumo e clique em **Concluir**.

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para o banco de dados SAP HANA

Você deve criar uma conexão de máquina virtual de armazenamento (SVM) e uma credencial antes de usar cmdlets do PowerShell para fazer backup, restaurar ou clonar bancos de dados SAP HANA.

Antes de começar

- Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.
- Você deve ter as permissões necessárias na função de administrador de infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estejam em andamento.

  As instalações do plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento porque o cache do host pode não ser atualizado e o status dos bancos de dados pode ser exibido na GUI do SnapCenter como “Não disponível para backup” ou "`Não no armazenamento NetApp ".

- Os nomes dos sistemas de armazenamento devem ser exclusivos.

  O SnapCenter não oferece suporte a vários sistemas de armazenamento com o mesmo nome em clusters diferentes. Cada sistema de armazenamento suportado pelo SnapCenter deve ter um nome exclusivo e um endereço IP LIF de dados exclusivo.

Passos

1. Inicie uma sessão de conexão do PowerShell usando o cmdlet Open-SmConnection.

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

2. Crie uma nova conexão com o sistema de armazenamento usando o cmdlet Add-SmStorageConnection.

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

3. Crie uma nova credencial usando o cmdlet Add-SmCredential.

   Este exemplo mostra como criar uma nova credencial chamada FinanceAdmin com credenciais do Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Adicione o host de comunicação SAP HANA ao SnapCenter Server.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode hana
```

5. Instale o pacote e o plug-in SnapCenter para banco de dados SAP HANA no host.

   Para Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
hana
```

   Para Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. Defina o caminho para o cliente HDBSQL.

   Para Windows:

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program
Files\sap\hdbclient\hdbsql.exe"}
```

   Para Linux:

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com
-PluginCode hana -configSettings
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup de bancos de dados SAP HANA

Se um recurso ainda não fizer parte de nenhum grupo de recursos, você poderá fazer backup do recurso na página Recursos.

Antes de começar

- Você deve ter criado uma política de backup.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.
- Para a operação de backup baseada em cópia de instantâneo, certifique-se de que todos os bancos de dados de locatários sejam válidos e ativos.
- Para criar backups de replicação do sistema SAP HANA, é recomendável adicionar todos os recursos do sistema SAP HANA em um grupo de recursos. Isso garante um backup perfeito durante o modo de failback de aquisição.

  "Crie grupos de recursos e anexe políticas" .

  "Fazer backup de grupos de recursos"

- Se você quiser criar um backup baseado em arquivo quando um ou mais bancos de dados de locatários estiverem inativos, defina o parâmetro ALLOW_FILE_BASED_BACKUP_IFINACTIVE_TENANTS_PRESENT como **YES** no arquivo de propriedades do HANA usando `Set-SmConfigSettings` cmdlet.

  As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando Get-Help *command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter"

- Para comandos pré e pós para operações de inatividade, instantâneo e retomada de atividade, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recurso, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Selecione * * e selecione o nome do host e o tipo de recurso para filtrar os recursos. Você pode então selecionar para fechar o painel de filtro.
3. Selecione o recurso que você deseja fazer backup.
4. Na página Recurso, selecione **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.
5. Na página Configurações do aplicativo, faça o seguinte:
   - Selecione a seta **Backups** para definir opções adicionais de backup:

     Habilite o backup do grupo de consistência, se necessário, e execute as seguintes tarefas:

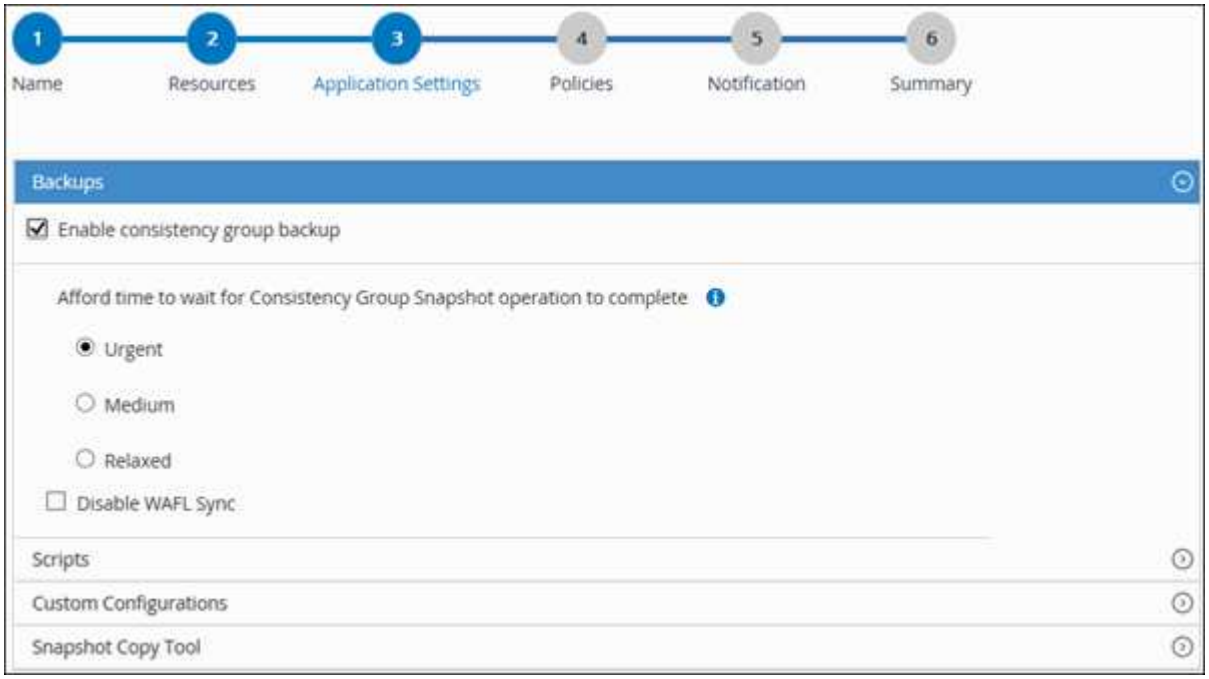
Para este campo…	Faça isso…
Permitir tempo para esperar a conclusão da operação "Consistency Group Snapshot"	Selecione **Urgente**, ou **Médio**, ou **Relaxado** para especificar o tempo de espera para a operação de Snapshot terminar. Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.
Desativar sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL .

   - Selecione a seta **Scripts** para executar comandos pré e pós para operações de inatividade, instantâneo e ativação/desativação.

     Você também pode executar pré-comandos antes de sair da operação de backup. Prescrições e pós-escritos são executados no SnapCenter Server.
   - Selecione a seta **Configurações personalizadas** e insira os pares de valores personalizados necessários para todos os trabalhos que usam este recurso.
   - Selecione a seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar Instantâneos:

Se você quiser…	Então…
SnapCenter para criar um Snapshot de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.

Se você quiser…	Então…
SnapCenter para usar o plug-in para Windows para colocar o sistema de arquivos em um estado consistente e, em seguida, criar um Snapshot	Selecione * SnapCenter com consistência do sistema de arquivos*.
Para inserir o comando para criar um Snapshot	Selecione **Outro** e insira o comando para criar um Snapshot.



6. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em * + *.

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Selecione * + * na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

   c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione **OK**.

      policy_name é o nome da política que você selecionou.

   Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

7. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. O SMTP também deve ser configurado em **Configurações** > **Configurações globais**.

8. Revise o resumo e selecione **Concluir**.

   A página de topologia de recursos é exibida.

9. Selecione **Fazer backup agora**.
10. Na página Backup, execute as seguintes etapas:
    a. Se você aplicou várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

       Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

    b. Selecione **Backup**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.
    - Nas configurações do MetroCluster , o SnapCenter pode não conseguir detectar um relacionamento de proteção após um failover.

      Para mais informações, consulte: "Não é possível detectar o relacionamento SnapMirror ou SnapVault após failover do MetroCluster"

    - Se você estiver fazendo backup de dados do aplicativo em VMDKs e o tamanho do heap Java para o SnapCenter Plug-in for VMware vSphere não for grande o suficiente, o backup poderá falhar.

      Para aumentar o tamanho do heap Java, localize o arquivo de script */opt/netapp/init_scripts/scvservice*. Nesse script, o comando *do_start method* inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: *Java -jar -Xmx8192M -Xms4096M*

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

   ```
   Open-smconnection  -SMSbaseurl
   https:\\snapctr.demo.netapp.com:8146\
   ```

   O prompt de nome de usuário e senha é exibido.

2. Adicione recursos usando o cmdlet Add-SmResources.

   Este exemplo mostra como adicionar um banco de dados SAP HANA do tipo SingleContainer:

```
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_'
```

Este exemplo mostra como adicionar um banco de dados SAP HANA do tipo MultipleContainers:

```
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'
```

Este exemplo mostra como criar um recurso de volume não relacionado a dados:

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Crie uma política de backup usando o cmdlet Add-SmPolicy.

   Este exemplo cria uma política de backup para um backup baseado em cópia de instantâneo:

   ```
   C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType
   Backup -PluginPolicyType hana -BackupType SnapShotBasedBackup
   ```

   Este exemplo cria uma política de backup para um backup baseado em arquivo:

   ```
   C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
   -PluginPolicyType hana -BackupType FileBasedBackup
   ```

4. Proteja o recurso ou adicione um novo grupo de recursos ao SnapCenter usando o cmdlet Add-SmResourceGroup.

   Este exemplo protege um único recurso de contêiner:

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

Este exemplo protege um recurso de vários contêineres:

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="MDC\SID"}
-Description test -usesnapcenterwithoutfilesystemconsistency
```

Este exemplo cria um novo grupo de recursos com a política e os recursos especificados:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sccore.test.com";"Uid"="SID"},@{"Host"="sc
corelinux62.sccore.test.com";"Uid"="MDC\SID"})
  -Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency  -plugincode 'HANA'
```

Este exemplo cria um grupo de recursos de volume sem dados:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="H11";"PluginName"=
"hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"Pl
uginName"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="No
nDataVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

5. Inicie uma nova tarefa de backup usando o cmdlet New-SmBackup.

   Este exemplo mostra como fazer backup de um grupo de recursos:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

   Este exemplo faz backup de um recurso protegido:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
-Policy hana_Filebased
```

6. Monitore o status do trabalho (em execução, concluído ou com falha) usando o cmdlet Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Monitore os detalhes do trabalho de backup, como ID do backup, nome do backup para executar a operação de restauração ou clonagem usando o cmdlet Get-SmBackupReport.

```
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 :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup de grupos de recursos

Um grupo de recursos é uma coleção de recursos em um host. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos.

Antes de começar

- Você deve ter criado um grupo de recursos com uma política anexada.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.

Sobre esta tarefa

Você pode fazer backup de um grupo de recursos sob demanda na página Recursos. Se um grupo de recursos tiver uma política anexada e um agendamento configurado, os backups ocorrerão automaticamente de acordo com o agendamento.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.

   Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou selecionando e, em seguida, selecionando a tag. Você pode então selecionar para fechar o painel de filtro.

3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e selecione **Fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
   a. Se você associou várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

      Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

   b. Selecione **Backup**.
5. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Monitorar operações de backup de bancos de dados SAP HANA

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Talvez você queira verificar o progresso para determinar quando ele foi concluído ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado correspondente das operações:

-

Em andamento

- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **Trabalhos**.
3. Na página Trabalhos, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de backup sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Backup**.
   d. No menu suspenso **Status**, selecione o status do backup.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione uma tarefa de backup e clique em **Detalhes** para visualizar os detalhes da tarefa.

   Embora o status do trabalho de backup seja exibido , ao clicar em detalhes do trabalho, você poderá ver que algumas das tarefas filhas da operação de backup ainda estão em andamento ou marcadas com sinais de alerta.

5. Na página Detalhes do trabalho, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Monitore as operações de proteção de dados em bancos de dados SAP HANA no painel Atividade

O painel Atividade exibe as cinco operações mais recentes realizadas. O painel Atividade também exibe quando a operação foi iniciada e o status da operação.

O painel Atividade exibe informações sobre operações de backup, restauração, clonagem e backup agendado.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Clique no painel Atividade para visualizar as cinco operações mais recentes.

   Quando você clica em uma das operações, os detalhes da operação são listados na página **Detalhes do trabalho**.

Cancelar operações de backup para SAP HANA

Você pode cancelar operações de backup que estão na fila.

O que você vai precisar

- Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de backup em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** fica desabilitado para operações que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de backup enfileiradas de outros membros enquanto estiver usando essa função.

Passos

1. Execute uma das seguintes ações:

Do…	Ação
Página do monitor	a. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. b. Selecione a operação e clique em **Cancelar trabalho**.
Painel de atividades	a. Após iniciar a operação de backup, clique em * * no painel Atividade para visualizar as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

A operação é cancelada e o recurso é revertido ao estado anterior.

Visualize backups e clones do banco de dados SAP HANA na página Topologia

Ao se preparar para fazer backup ou clonar um recurso, pode ser útil visualizar uma representação gráfica de todos os backups e clones no armazenamento primário e secundário.

Sobre esta tarefa

Você pode revisar os seguintes ícones na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no armazenamento primário ou secundário (cópias espelhadas ou cópias do Vault).

-  exibe o número de backups e clones que estão disponíveis no armazenamento primário.
-

 exibe o número de backups e clones que são espelhados no armazenamento secundário usando a tecnologia SnapMirror .

-  exibe o número de backups e clones que são replicados no armazenamento secundário usando a tecnologia SnapVault .

> O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou 6 backups usando uma política para manter apenas 4 backups, o número de backups exibidos será 6.

> Clones de um backup de um espelho flexível em termos de versão em um volume do tipo mirror-vault são exibidos na exibição de topologia, mas a contagem de backups de espelho na exibição de topologia não inclui o backup flexível em termos de versão.

Na página Topologia, você pode ver todos os backups e clones disponíveis para o recurso ou grupo de recursos selecionado. Você pode visualizar os detalhes desses backups e clones e selecioná-los para executar operações de proteção de dados.

Se você tiver um relacionamento secundário como sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC]), poderá ver os seguintes ícones adicionais:

-  O site de réplica está no ar.
-  O site de réplicas está fora do ar.
-  O espelho secundário ou o relacionamento do cofre não foram restabelecidos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso na exibição de detalhes do recurso ou na exibição de detalhes do grupo de recursos.

   Se o recurso estiver protegido, a página de topologia do recurso selecionado será exibida.

4. Revise o **cartão Resumo** para ver um resumo do número de backups e clones disponíveis no armazenamento primário e secundário.

   A seção **Cartão de resumo** exibe o número total de backups baseados em arquivo, backups baseados em cópia de instantâneo e clones.

   Clicar no botão **Atualizar** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clicar no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Uma programação semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo estiver distribuído em vários volumes, o tempo de expiração do SnapLock

para o backup será o maior tempo de expiração do SnapLock definido para um Snapshot em um volume. O maior tempo de expiração do SnapLock é recuperado do ONTAP.

Para sincronização ativa do SnapMirror , clicar no botão **Atualizar** atualiza o inventário de backup do SnapCenter consultando o ONTAP para sites primários e de réplica. Uma programação semanal também executa essa atividade para todos os bancos de dados que contêm o relacionamento de sincronização ativo do SnapMirror .

- Para sincronização ativa do SnapMirror e somente para o ONTAP 9.14.1, os relacionamentos Async Mirror ou Async MirrorVault com o novo destino primário devem ser configurados manualmente após o failover. A partir do ONTAP 9.15.1, o Async Mirror ou o Async MirrorVault são configurados automaticamente para o novo destino principal.
- Após o failover, um backup deve ser criado para que o SnapCenter esteja ciente do failover. Você pode clicar em **Atualizar** somente após um backup ter sido criado.

5. Na exibição Gerenciar cópias, clique em **Backups** ou **Clones** do armazenamento primário ou secundário para ver detalhes de um backup ou clone.

   Os detalhes dos backups e clones são exibidos em formato de tabela.

6. Selecione o backup na tabela e clique nos ícones de proteção de dados para executar operações de restauração, clonagem e exclusão.

   Não é possível renomear ou excluir backups que estejam no armazenamento secundário.

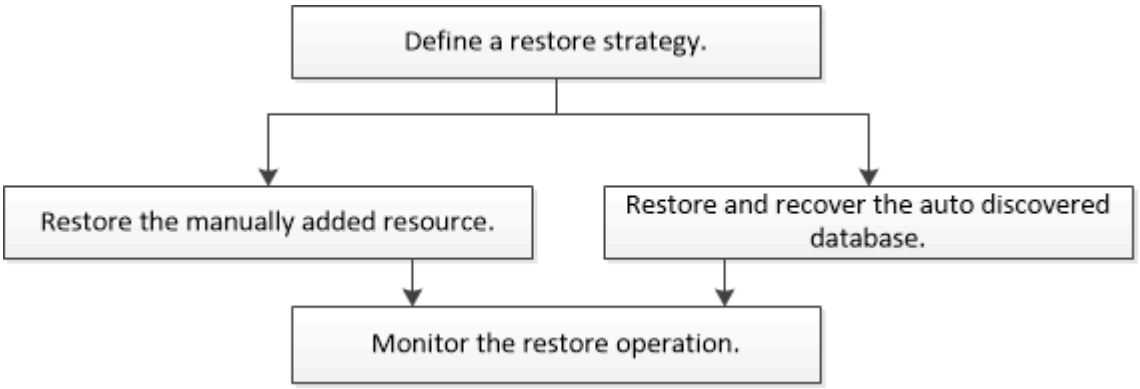
7. Se você quiser excluir um clone, selecione o clone na tabela e clique em .
8. Se você quiser dividir um clone, selecione o clone na tabela e clique em .

Restaurar bancos de dados SAP HANA

Fluxo de trabalho de restauração

O fluxo de trabalho de restauração e recuperação inclui planejamento, execução de operações de restauração e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de restauração:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre os cmdlets do PowerShell.

"Guia de referência do cmdlet do software SnapCenter" .

Restaurar e recuperar um backup de recurso adicionado manualmente

Você pode usar o SnapCenter para restaurar e recuperar dados de um ou mais backups.

Antes de começar

- Você deve ter feito backup do recurso ou dos grupos de recursos.
- Você deve ter cancelado qualquer operação de backup que esteja em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos de pré-restauração, pós-restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Cópias de backup baseadas em arquivo não podem ser restauradas do SnapCenter.
- Após a atualização para o SnapCenter 4.3, os backups feitos no SnapCenter 4.2 podem ser restaurados, mas não podem ser recuperados. Você deve usar o HANA Studio ou scripts de recuperação do HANA externos ao SnapCenter para recuperar os backups feitos no SnapCenter 4.2.
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .
- Para a operação de restauração de sincronização ativa do SnapMirror , você deve selecionar o backup do local principal.

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com o tipo, host, grupos de recursos e políticas associados e status.

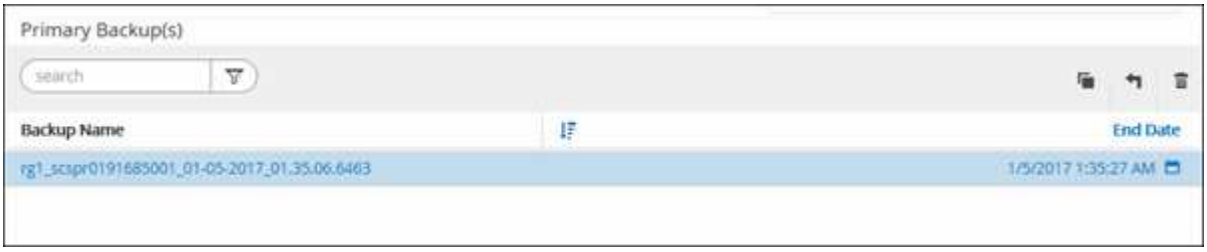
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, "Não protegido" será exibido na coluna Status geral. Isso pode significar que o recurso não está protegido ou que o backup do recurso foi feito por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e depois selecione um recurso nesse grupo.

   A página de topologia de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela Backup(s) primário(s), selecione o backup que deseja restaurar e clique em * * .



6. Na página Escopo de restauração, selecione **Recurso completo** ou **Nível de arquivo**.

   a. Se você selecionar **Recurso Completo**, todos os volumes de dados configurados do banco de dados SAP HANA serão restaurados.

      Se o recurso contiver volumes ou qtrees, os Snapshots tirados após o Snapshot selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

   b. Se você selecionar **Nível de arquivo**, poderá selecionar **Todos** ou selecionar os volumes ou qtrees específicos e, em seguida, inserir o caminho relacionado a esses volumes ou qtrees, separados por vírgulas

      - Você pode selecionar vários volumes e qtrees.
      - Se o tipo de recurso for LUN, todo o LUN será restaurado.

        Você pode selecionar vários LUNs.

   Se você selecionar **Todos**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.

7. Na página Pré-operações, insira os comandos pre restore e unmount para executar antes de realizar um trabalho de restauração.

   Os comandos de desmontagem não estão disponíveis para recursos descobertos automaticamente.

8. Na página Post ops, insira os comandos mount e post restore para serem executados após realizar um trabalho de restauração.

   Os comandos de montagem não estão disponíveis para recursos descobertos automaticamente.

9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O SMTP também deve ser configurado na página **Configurações** > **Configurações globais**.

10. Revise o resumo e clique em **Concluir**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
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
```

   Este exemplo exibe informações detalhadas sobre o backup de 29 de janeiro de 2015 a 3 de fevereiro de 2015:

```
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. Restaure os dados do backup usando o cmdlet Restore-SmBackup.

```
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          :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Restaurar e recuperar um backup de banco de dados descoberto automaticamente

Você pode usar o SnapCenter para restaurar e recuperar dados de um ou mais backups.

Antes de começar

- Você deve ter feito backup do recurso ou dos grupos de recursos.
- Você deve ter cancelado qualquer operação de backup que esteja em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos de pré-restauração, pós-restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-*

in Creator\etc\allowed_commands.config

- Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Cópias de backup baseadas em arquivo não podem ser restauradas do SnapCenter.
- Após a atualização para o SnapCenter 4.3, os backups feitos no SnapCenter 4.2 podem ser restaurados, mas não podem ser recuperados. Você deve usar o HANA Studio ou scripts de recuperação do HANA externos ao SnapCenter para recuperar os backups feitos no SnapCenter 4.2.
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .
- Para a operação de restauração de sincronização ativa do SnapMirror , você deve selecionar o backup do local principal.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com o tipo, host, grupos de recursos e políticas associados e status.

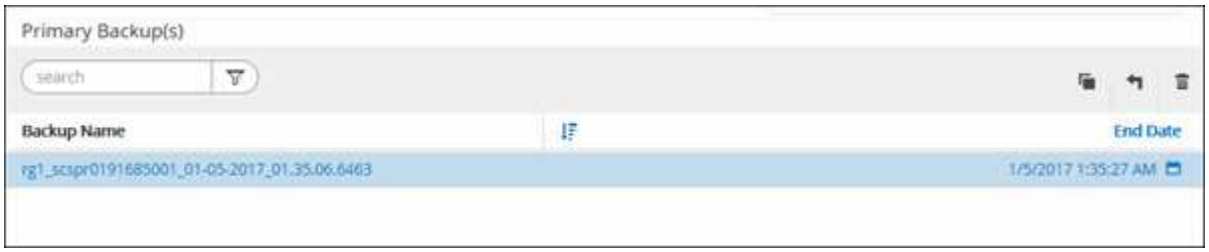
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, “Não protegido” será exibido na coluna Status geral. Isso pode significar que o recurso não está protegido ou que o backup do recurso foi feito por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e depois selecione um recurso nesse grupo.

   A página de topologia de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela Backup(s) primário(s), selecione o backup que deseja restaurar e clique em * ↰ *.



6. Na página Restaurar Escopo, selecione **Recurso Completo** para restaurar os volumes de dados configurados do banco de dados SAP HANA.

   Você pode selecionar **Recurso Completo** (com ou sem **Reversão de Volume**) ou **Banco de Dados de Locatários**.

A operação de recuperação não é suportada pelo SnapCenter Server para vários locatários quando o usuário seleciona a opção **Banco de dados de locatários** ou **Restauração completa**. Você deve usar o HANA Studio ou o script HANA Python para executar a operação de recuperação.

a. Selecione **Reverter Volume** se quiser restaurar o volume inteiro.

   Esta opção está disponível para backups feitos no SnapCenter 4.3 em ambientes NFS.

   Se o recurso contiver volumes ou qtrees, os Snapshots tirados após o Snapshot selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído. Isso é aplicável quando a opção **Recurso Completo** com **Reversão de Volume** é selecionada para restauração.

b. Selecione **Banco de dados de locatários**.

   Esta opção está disponível somente para recursos do MDC.

   Certifique-se de parar o banco de dados do locatário antes de executar a operação de restauração.

Se você selecionar a opção **Banco de dados de locatários**, deverá usar o HANA Studio ou usar scripts de recuperação do HANA externos ao SnapCenter para executar a operação de recuperação.

7. Na página Escopo de recuperação, selecione uma das seguintes opções:

Se você…	Faça isso…
Quer recuperar o mais próximo possível do tempo atual	Selecione **Recuperar para o estado mais recente**. Para recursos de contêiner único, especifique um ou mais locais de backup de log e catálogo. Para recursos de contêiner de banco de dados multilocatário (MDC), especifique um ou mais locais de backup de log e o local do catálogo de backup. Para recursos do MDC, o caminho deve conter logs do banco de dados do sistema e do banco de dados do locatário.

Se você…	Faça isso…
Deseja recuperar até o ponto especificado no tempo	Selecione **Recuperar para um ponto no tempo**. a. Selecione o fuso horário. O fuso horário do navegador é preenchido por padrão. O fuso horário selecionado, juntamente com o horário de entrada, é convertido para GMT absoluto. b. Insira a data e a hora. Por exemplo, o host HANA Linux está localizado em Sunnyvale, CA, e o usuário em Raleigh, NC, está recuperando os logs no SnapCenter. A diferença de horário entre esses dois locais é de 3 horas e, como o usuário fez login em Raleigh, Carolina do Norte, o fuso horário padrão do navegador que será selecionado na GUI é GMT-04:00. Se o usuário quiser executar uma recuperação para 5h da manhã em Sunnyvale, CA, o usuário deverá definir o fuso horário do navegador para o fuso horário do host HANA Linux, que é GMT-07:00 e especificar a data e a hora como 5h da manhã. Para recursos de contêiner único, especifique um ou mais locais de backup de log e catálogo. Para recursos do MDC, especifique um ou mais locais de backup de log e o local do catálogo de backup. Para recursos do MDC, o caminho deve conter logs do banco de dados do sistema e do banco de dados do locatário.
Deseja recuperar um backup de dados específico	Selecione **Recuperar para backup de dados especificado**.
Não quero recuperar	Selecione **Sem recuperação**. Você deve executar a operação de recuperação manualmente no estúdio HANA.

Você pode recuperar somente os backups feitos após a atualização para o SnapCenter 4.3, desde que o host e o plug-in sejam atualizados para o SnapCenter 4.3 e os backups selecionados para restauração sejam feitos após o recurso ser convertido ou descoberto como recurso descoberto automaticamente.

8. Na página Pré-operações, insira os comandos pre restore e unmount para executar antes de realizar um trabalho de restauração.

   Os comandos de desmontagem não estão disponíveis para recursos descobertos automaticamente.

9. Na página Post ops, insira os comandos mount e post restore para serem executados após realizar um trabalho de restauração.

   Os comandos de montagem não estão disponíveis para recursos descobertos automaticamente.

10. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

    Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O SMTP também deve ser configurado na página **Configurações** > **Configurações globais**.

11. Revise o resumo e clique em **Concluir**.
12. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Restaurar recursos usando cmdlets do PowerShell

Restaurar um backup de recursos inclui iniciar uma sessão de conexão com o SnapCenter Server, listar os backups e recuperar informações de backup, além de restaurar um backup.

Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
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
```

Este exemplo exibe informações detalhadas sobre o backup de 29 de janeiro de 2015 a 3 de fevereiro de 2015:

```
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. Restaure os dados do backup usando o cmdlet Restore-SmBackup.

```
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          :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitorar operações de restauração de bancos de dados SAP HANA

Você pode monitorar o progresso de diferentes operações de restauração do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa tomar.

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento

- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de restauração sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Restaurar**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Aplicar** para visualizar as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Clonar backups de recursos do SAP HANA

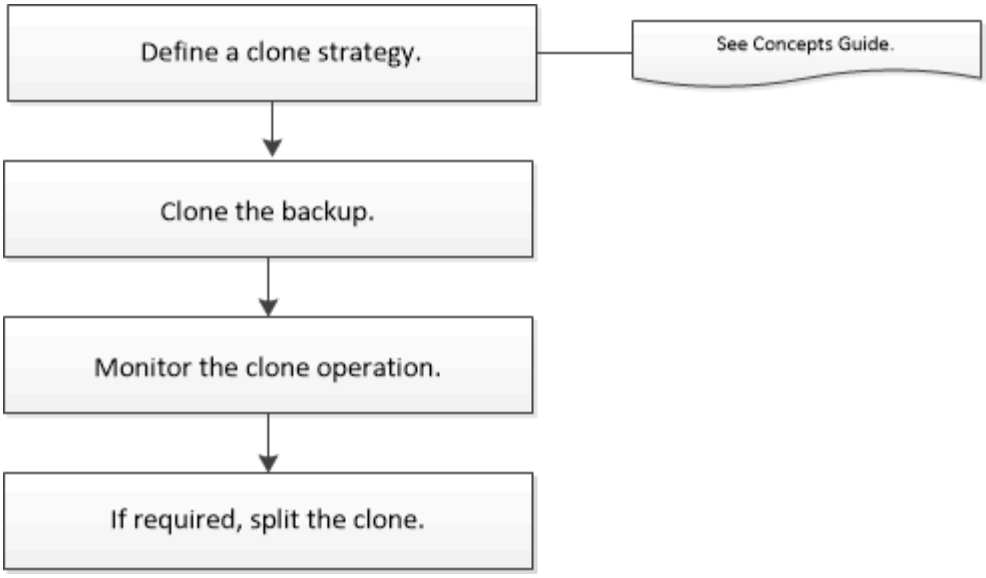
Fluxo de trabalho de clonagem

O fluxo de trabalho de clonagem inclui executar a operação de clonagem e monitorar a operação.

Sobre esta tarefa

- Você pode clonar no servidor SAP HANA de origem.
- Você pode clonar backups de recursos pelos seguintes motivos:
  - Para testar a funcionalidade que deve ser implementada usando a estrutura e o conteúdo atuais dos recursos durante os ciclos de desenvolvimento do aplicativo
  - Para ferramentas de extração e manipulação de dados ao preencher data warehouses
  - Para recuperar dados que foram excluídos ou alterados por engano

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de clonagem:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre os cmdlets do PowerShell.

Clonar um backup de banco de dados SAP HANA

Você pode usar o SnapCenter para clonar um backup. Você pode clonar a partir do backup primário ou secundário.

Antes de começar

- Você deve ter feito backup dos recursos ou do grupo de recursos.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de armazenamento (SVM).
- Não é possível clonar backups baseados em arquivos.
- O servidor clone de destino deve ter o mesmo SID de instância do SAP HANA fornecido no campo SID do clone de destino.
- Para comandos de pré-clonagem ou pós-clonagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Para Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Para Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Para obter informações sobre as limitações da operação de divisão de clones, consulte "Guia de gerenciamento de armazenamento lógico ONTAP 9" .
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos Snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com informações como tipo, host, grupos de recursos e políticas associados e status.

3. Selecione o recurso ou grupo de recursos.

   Você deve selecionar um recurso se selecionar um grupo de recursos.

   A página de topologia de recurso ou grupo de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Selecione o backup de dados da tabela e clique em  .
6. Na página Localização, execute as seguintes ações:

Para este campo…	Faça isso…
Host de plug-in	Selecione o host no qual o clone deve ser montado e o plug-in será instalado.
SID do clone de destino	Insira o ID da instância do SAP HANA a ser clonada dos backups existentes.
Endereço IP de exportação NFS	Insira os endereços IP ou os nomes de host nos quais os volumes clonados serão exportados.
Iniciador iSCSI	Digite o nome do iniciador iSCSI do host para o qual os LUNs são exportados. Esta opção só estará disponível se você selecionar o tipo de recurso LUN.
Protocolo	Digite o protocolo LUN. Esta opção só estará disponível se você selecionar o tipo de recurso LUN.

   Se o recurso selecionado for um LUN e você estiver clonando de um backup secundário, os volumes de destino serão listados. Uma única origem pode ter vários volumes de destino.

   Antes de clonar, você deve garantir que o iniciador iSCSI ou o FCP esteja presente, configurado e conectado em hosts alternativos.

7. Na página Scripts, execute as seguintes etapas:

   Os scripts são executados no host do plug-in.

a. Insira os comandos para pré-clonagem ou pós-clonagem que devem ser executados antes ou depois da operação de clonagem, respectivamente.
   - Comando pré-clone: exclui bancos de dados existentes com o mesmo nome
   - Comando post clone: verifica um banco de dados ou inicia um banco de dados.

b. Digite o comando mount para montar um sistema de arquivos em um host.

   Comando de montagem para um volume ou qtree em uma máquina Linux:

Exemplo para NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail.

9. Revise o resumo e clique em **Concluir**.
10. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

2. Recupere os backups para executar a operação de clonagem usando o cmdlet Get-SmBackup.

   Este exemplo mostra que dois backups estão disponíveis para clonagem:

```
 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. Inicie uma operação de clonagem a partir de um backup existente e especifique os endereços IP de exportação do NFS nos quais os volumes clonados serão exportados.

   Este exemplo mostra que o backup a ser clonado tem um endereço NFSExportIPs de 10.232.206.169:

```
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
shivscc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data'
-preclonecreatecommands '/home/scripts/scpre_clone.sh'
-postclonecreatecommands '/home/scripts/scpost_clone.sh'
```

Se NFSExportIPs não for especificado, o padrão será exportado para o host de destino do clone.

4. Verifique se os backups foram clonados com sucesso usando o cmdlet Get-SmCloneReport para visualizar os detalhes do trabalho de clonagem.

   Você pode visualizar detalhes como ID do clone, data e hora de início, data e hora de término.

```
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          :
```

Monitorar operações de clonagem de banco de dados SAP HANA

Você pode monitorar o progresso das operações de clonagem do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para

determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente operações de clonagem sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione o trabalho de clonagem e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página Detalhes do trabalho, clique em **Exibir registros**.

Dividir um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido se torna independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clone em um clone intermediário.

  Por exemplo, depois de criar o clone1 a partir de um backup de banco de dados, você pode criar um backup do clone1 e então clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e você não pode executar a operação de divisão de clone no clone1. No entanto, você pode executar a operação de divisão de clone no clone2.

  Após dividir o clone2, você pode executar a operação de divisão do clone no clone1 porque o clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e os trabalhos de clonagem do clone são excluídos.
- Para obter informações sobre as operações de divisão de volume do FlexClone , consulte "Dividir um volume FlexClone de seu volume pai" .

- Certifique-se de que o volume ou agregado no sistema de armazenamento esteja online.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página **Recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicações de banco de dados	Selecione **Banco de dados** na lista Exibir.
Para sistemas de arquivos	Selecione **Caminho** na lista Exibir.

3. Selecione o recurso apropriado na lista.

   A página de topologia de recursos é exibida.

4. Na exibição **Gerenciar cópias**, selecione o recurso clonado (por exemplo, o banco de dados ou LUN) e clique em *  *.
5. Revise o tamanho estimado do clone que será dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

   A operação de divisão do clone para de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clone e, em seguida, tentar novamente a operação de divisão de clone.

   Se você quiser um tempo de pesquisa maior ou menor para verificar se o clone está dividido ou não, você pode alterar o valor do parâmetro *CloneSplitStatusCheckPollTime* no arquivo *SMCoreServiceHost.exe.config* para definir o intervalo de tempo para o SMCore pesquisar o status da operação de divisão do clone. O valor está em milissegundos e o valor padrão é 5 minutos.

   Por exemplo:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   A operação de início da divisão do clone falha se um backup, uma restauração ou outra divisão do clone estiver em andamento. Você deve reiniciar a operação de divisão do clone somente após a conclusão das operações em execução.

Informações relacionadas

"O clone ou a verificação do SnapCenter falham com o agregado inexistente"

Excluir ou dividir clones de banco de dados SAP HANA após atualizar o SnapCenter

Após atualizar para o SnapCenter 4.3, você não verá mais os clones. Você pode excluir o clone ou dividir os clones na página Topologia do recurso a partir do qual os clones foram criados.

Sobre esta tarefa

Se você quiser localizar a pegada de armazenamento dos clones ocultos, execute o seguinte comando: `Get-SmClone -ListStorageFootprint`

Passos

1. Exclua os backups dos recursos clonados usando o cmdlet remove-smbackup.
2. Exclua o grupo de recursos dos recursos clonados usando o cmdlet remove-smresourcegroup.
3. Remova a proteção do recurso clonado usando o cmdlet remove-smprotectresource.
4. Selecione o recurso pai na página Recursos.

   A página de topologia de recursos é exibida.

5. Na exibição Gerenciar cópias, selecione os clones dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
6. Selecione os clones e clique em para excluir clones ou clicar para dividir os clones.
7. Clique em **OK**.

Proteja bancos de dados Oracle

Visão geral do plug-in SnapCenter para banco de dados Oracle

O que você pode fazer com o Plug-in para Oracle Database

O SnapCenter Plug-in para Oracle Database é um componente do lado do host do NetApp SnapCenter Software que permite o gerenciamento de proteção de dados com reconhecimento de aplicativo de bancos de dados Oracle.

O plug-in para Oracle Database automatiza o backup, a catalogação e a descatalogação com o Oracle Recovery Manager (RMAN), a verificação, a montagem, a desmontagem, a restauração, a recuperação e a clonagem de bancos de dados Oracle no seu ambiente SnapCenter . O Plug-in para Oracle Database instala o SnapCenter Plug-in para UNIX para executar todas as operações de proteção de dados.

Você pode usar o Plug-in para Oracle Database para gerenciar backups de bancos de dados Oracle executando aplicativos SAP. Entretanto, a integração do SAP BR*Tools não é suportada.

- Faça backup de arquivos de dados, arquivos de controle e arquive arquivos de log.

  O backup é suportado apenas no nível do banco de dados de contêiner (CDB).

- Restauração e recuperação de bancos de dados, CDBs e bancos de dados plugáveis (PDBs).

  A recuperação incompleta de PDBs não é suportada.

- Crie clones de bancos de dados de produção até um determinado momento.

  A clonagem é suportada apenas no nível CDB.

- Verifique os backups imediatamente.
- Monte e desmonte backups de dados e logs para operação de recuperação.
- Agende operações de backup e verificação.
- Monitore todas as operações.
- Visualize relatórios de operações de backup, restauração e clonagem.
- Automatiza operações de backup, restauração, recuperação, verificação, montagem, desmontagem e clonagem com reconhecimento de aplicativo para bancos de dados Oracle em seu ambiente SnapCenter
- Suporta bancos de dados Oracle para SAP, no entanto, a integração com SAP BR*Tools não é fornecida

Recursos do Plug-in para Oracle Database

O plug-in para Oracle Database integra-se ao banco de dados Oracle no host Linux ou AIX e às tecnologias NetApp no sistema de armazenamento.

- Interface gráfica de usuário unificada

  A interface do SnapCenter fornece padronização e consistência entre plug-ins e ambientes. A interface do SnapCenter permite que você conclua operações consistentes de backup, restauração, recuperação e

clonagem em plug-ins, use relatórios centralizados, use visualizações de painel rápidas, configure o controle de acesso baseado em função (RBAC) e monitore trabalhos em todos os plug-ins.

- Administração central automatizada

  Você pode agendar operações de backup e clonagem, configurar retenção de backup baseada em políticas e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- Tecnologia NetApp Snapshot não disruptiva

  O SnapCenter usa a tecnologia NetApp Snapshot com o Plug-in para Oracle Database e o Plug-in para UNIX para fazer backup de bancos de dados. Os instantâneos consomem espaço de armazenamento mínimo.

O Plug-in para Oracle Database também oferece os seguintes benefícios:

- Suporte para fluxos de trabalho de backup, restauração, clonagem, montagem, desmontagem e verificação
- Descoberta automática de bancos de dados Oracle configurados no host
- Suporte para catalogação e descatalogação usando o Oracle Recovery Manager (RMAN)
- Segurança com suporte RBAC e delegação centralizada de funções

  Você também pode definir as credenciais para que os usuários autorizados do SnapCenter tenham permissões no nível do aplicativo.

- Suporte para Archive Log Management (ALM) para operações de restauração e clonagem
- Criação de cópias de bancos de dados de produção com eficiência de espaço e em um determinado momento para testes ou extração de dados usando a tecnologia NetApp FlexClone

  Uma licença FlexClone é necessária no sistema de armazenamento onde você deseja criar o clone.

- Suporte para o recurso de grupo de consistência (CG) do ONTAP como parte da criação de backups em ambientes SAN e ASM
- Verificação de backup automatizada e sem interrupções
- Capacidade de executar vários backups simultaneamente em vários hosts de banco de dados

  Em uma única operação, os Snapshots são consolidados quando bancos de dados em um único host compartilham o mesmo volume.

- Suporte para infraestruturas físicas e virtualizadas
- Suporte para NFS, iSCSI, Fibre Channel (FC), RDM, VMDK sobre NFS e VMFS, e ASM sobre NFS, SAN, RDM e VMDK
- Suporte para o recurso Selective LUN Map (SLM) do ONTAP

  Habilitado por padrão, o recurso SLM descobre periodicamente os LUNs que não têm caminhos otimizados e os corrige. Você pode configurar o SLM modificando os parâmetros no arquivo scu.properties localizado em /var/opt/snapcenter/scu/etc.

  - Você pode desabilitar isso definindo o valor do parâmetro ENABLE_LUNPATH_MONITORING como falso.

- Você pode especificar a frequência com que os caminhos LUN serão corrigidos automaticamente atribuindo o valor (em horas) ao parâmetro LUNPATH_MONITORING_INTERVAL. Para obter informações sobre SLM, consulte o "Seção de administração do ONTAP 9 SAN" .

- Suporte para memória não volátil expressa (NVMe) no Linux
  - O utilitário NVMe deve ser instalado no host.

    Você deve instalar o utilitário NVMe para clonar ou montar em um host alternativo.
  - As operações de backup, restauração, clonagem, montagem, desmontagem, catalogação, descatalogação e verificação são suportadas no hardware NVMe, exceto para ambientes virtualizados como RDM.

    As operações acima são suportadas em dispositivos sem partições ou com partição única.

    > Você pode configurar uma solução de multicaminho para dispositivos NVMe definindo a opção de multicaminho nativa no kernel. O multipathing do Device Mapper (DM) não é suportado.

  - Os fluxos de trabalho de backup, restauração, clonagem, montagem, desmontagem, catalogação, descatalogação e verificação são suportados no NVMe sobre TCP/IP.
  - Os fluxos de trabalho de backup, restauração, clonagem, montagem, desmontagem, catalogação, descatalogação e verificação são suportados no layout VMDK criado em NVMe sobre TCP/IP.
- Oferece suporte à sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC]), que permite que os serviços empresariais continuem operando mesmo durante uma falha completa do site, permitindo que os aplicativos façam failover de forma transparente usando uma cópia secundária. Não é necessária intervenção manual nem script adicional para acionar um failover com a sincronização ativa do SnapMirror .
- Suporta qualquer usuário não padrão em vez de Oracle e Grid.

  Para oferecer suporte aos usuários não padrão, você deve defini-los modificando os valores dos parâmetros no arquivo **sco.properties** localizado em *file /var/opt/snapcenter/sco/etc/*.

  Os valores padrão dos parâmetros são definidos como oracle e grid.
  - DB_USER=oráculo
  - DB_GROUP=oinstall
  - GI_USER=grade
  - GI_GROUP=oinstall

Tipos de armazenamento suportados pelo Plug-in para Oracle Database

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e virtuais. Você deve verificar o suporte para seu tipo de armazenamento antes de instalar o Pacote de plug-ins SnapCenter para Linux ou o Pacote de plug-ins SnapCenter para AIX.

O SnapCenter não oferece suporte ao provisionamento de armazenamento para Linux e AIX.

Tipos de armazenamento suportados no Linux

A tabela a seguir lista os tipos de armazenamento suportados no Linux.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados por FC • LUNs conectados por iSCSI • Volumes conectados ao NFS • NVMe-FC • NVMe/TCP
VMware ESXi	• LUNs RDM conectados por um FC ou iSCSI ESXi HBAA varredura de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluída porque o SnapCenter verifica todos os adaptadores de barramento de host presentes no host. Você pode editar o arquivo **LinuxConfig.pm** localizado em */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* para definir o valor do parâmetro **SCSI_HOSTS_OPTIMIZED_RESCAN** como 1 para verificar novamente apenas os HBAs listados em HBA_DRIVER_NAMES. • LUNs iSCSI conectados diretamente ao sistema convidado pelo iniciador iSCSI • VMDKs em armazenamentos de dados NFS • VMDKs em VMFS criados sobre NVMe/TCP O RAC é suportado no ESX 8.0U2, que tem suporte para VMDK compartilhado • Volumes NFS conectados diretamente ao sistema convidado • Armazenamentos de dados vVol em NFS e SAN O armazenamento de dados vVol só pode ser provisionado com o ONTAP Tools para VMware vSphere.

Tipos de armazenamento suportados no AIX

A tabela a seguir lista os tipos de armazenamento suportados no AIX.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados por FC e iSCSI. Em um ambiente SAN, os sistemas de arquivos ASM, LVM e SAN são suportados. NFS no AIX e no sistema de arquivos não é suportado. • Sistema de Arquivos com Registro Aprimorado (JFS2) Suporta registro em linha em sistemas de arquivos SAN e layout LVM.

O "Ferramenta de Matriz de Interoperabilidade da NetApp" contém as informações mais recentes sobre as versões suportadas.

Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para Plug-in para Oracle

Você pode usar um plug-in SnapCenter com a tecnologia ONTAP SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia ONTAP SnapVault para executar replicação de backup de disco para disco para conformidade com padrões e outros propósitos relacionados à governança. Antes de executar essas tarefas, você deve configurar um relacionamento de proteção de dados entre os volumes de origem e destino e inicializar o relacionamento.

O SnapCenter executa as atualizações no SnapMirror e no SnapVault após concluir a operação Snapshot. As atualizações do SnapMirror e do SnapVault são executadas como parte do trabalho do SnapCenter ; não crie uma programação ONTAP separada.

Se você estiver acessando o SnapCenter a partir de um produto NetApp SnapManager e estiver satisfeito com os relacionamentos de proteção de dados configurados, pode pular esta seção.

Um relacionamento de proteção de dados replica dados do armazenamento primário (o volume de origem) para o armazenamento secundário (o volume de destino). Quando você inicializa o relacionamento, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não oferece suporte a relacionamentos em cascata entre volumes SnapMirror e SnapVault (**Primário** > **Espelho** > **Cofre**). Você deve usar relacionamentos fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis em termos de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis em termos de versão e como configurá-los, consulte "Documentação do ONTAP" .

Privilégios ONTAP mínimos necessários para o Plug-in para Oracle

Os privilégios mínimos do ONTAP necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

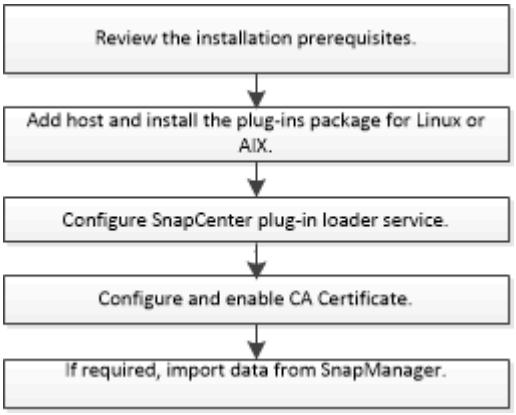
- Comandos de acesso total: privilégios mínimos necessários para ONTAP 9.12.1 e posterior
  - evento generate-autosupport-log
  - histórico de trabalho mostrar
  - parada de trabalho
  - lua
  - mostrar atributo lun
  - lun criar
  - lun delete
  - geometria lunar
  - lun igroup adicionar
  - lun igroup criar
  - lun igroup excluir
  - renomear lun igroup
  - show do lun igroup
  - mapeamento lun add-reporting-nodes
  - criação de mapeamento lun
  - exclusão de mapeamento lun
  - mapeamento lun remove-reporting-nodes
  - show de mapeamento lunar
  - lun modificar
  - volume de entrada lun
  - lua offline
  - lua online
  - lun persistente-reserva clara
  - redimensionamento de lun
  - série lun
  - show de lua
  - política de adição de regra do snapmirror
  - regra de modificação de política do snapmirror
  - política de remoção do snapmirror
  - política do snapmirror mostrar
  - restauração do snapmirror
  - show de espelhos instantâneos

- histórico de exibição do snapmirror
- atualização do snapmirror
- atualização do snapmirror-ls-set
- lista-destinos do snapmirror
- versão
- criação de clone de volume
- show de clones de volume
- volume clone split start
- volume clone divisão parada
- volume criar
- destruição de volume
- clone de arquivo de volume criar
- arquivo de volume mostrar-uso-do-disco
- volume offline
- volume on-line
- modificação de volume
- volume qtree criar
- volume qtree delete
- volume qtree modificar
- volume qtree mostrar
- restrição de volume
- show de volume
- criação de instantâneo de volume
- exclusão de instantâneo de volume
- modificação de instantâneo de volume
- renomeação de instantâneo de volume
- restauração de instantâneo de volume
- arquivo de restauração de instantâneo de volume
- exibição de instantâneo de volume
- desmontagem de volume
- vserver
- cifs do vserver
- vserver cifs shadowcopy mostrar
- vserver mostrar
- interface de rede
- exibição de interface de rede
- show do metrocluster

Instalar o plug-in SnapCenter para o banco de dados Oracle

Fluxo de trabalho de instalação do plug-in SnapCenter para Oracle Database

Você deve instalar e configurar o SnapCenter Plug-in para Oracle Database se quiser proteger bancos de dados Oracle.



Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Linux ou AIX

Antes de adicionar um host e instalar os pacotes de plug-ins, você deve atender a todos os requisitos.

- Se você estiver usando iSCSI, o serviço iSCSI deverá estar em execução.
- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.

  O plug-in SnapCenter para Oracle Database pode ser instalado por um usuário não root. No entanto, você deve configurar os privilégios sudo para que o usuário não root instale e inicie o processo do plug-in. Após instalar o plug-in, os processos serão executados como um usuário não root.

- Se estiver instalando o pacote de plug-ins SnapCenter para AIX no host AIX, você deverá ter resolvido manualmente os links simbólicos no nível do diretório.

  O pacote de plug-ins SnapCenter para AIX resolve automaticamente o link simbólico no nível do arquivo, mas não os links simbólicos no nível do diretório para obter o caminho absoluto JAVA_HOME.

- Crie credenciais com modo de autenticação como Linux ou AIX para o usuário de instalação.
- Você deve ter instalado o Java 11 no seu host Linux ou AIX.
  - Java da Oracle e OpenJDK são suportados para Linux
  - IBM Java para AIX. Você pode baixar de "Downloads do IBM Semeru Runtimes"

    Certifique-se de ter instalado apenas a edição certificada do JAVA 11 no host Linux.

- Para bancos de dados Oracle em execução em um host Linux ou AIX, você deve instalar o SnapCenter Plug-in para Oracle Database e o SnapCenter Plug-in para UNIX.

Você também pode usar o Plug-in para Oracle Database para gerenciar bancos de dados Oracle para SAP. Entretanto, a integração do SAP BR*Tools não é suportada.

- Se estiver usando o banco de dados Oracle 11.2.0.3 ou posterior, você deverá instalar o patch 13366202 do Oracle.

O mapeamento de UUID no arquivo /etc/fstab não é suportado pelo SnapCenter.

- Você deve ter **bash** como o shell padrão para instalação de plug-ins.

Requisitos do host Linux

Você deve garantir que o host atenda aos requisitos antes de instalar o Pacote de plug-ins do SnapCenter para Linux.

Item	Requisitos
Sistemas operacionais	• Red Hat Enterprise Linux • Oracle Linux Se você estiver usando o banco de dados Oracle no LVM nos sistemas operacionais Oracle Linux ou Red Hat Enterprise Linux 6.6 ou 7.0, deverá instalar a versão mais recente do Logical Volume Manager (LVM). • Servidor SUSE Linux Enterprise (SLES)
RAM mínima para o plug-in SnapCenter no host	2 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	2 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.

Item	Requisitos
Pacotes de software necessários	Java 11 Oracle e OpenJDK Certifique-se de ter instalado apenas a edição certificada do JAVA 11 no host Linux. Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em /var/opt/snapcenter/spl/etc/spl.properties esteja definida para a versão correta do JAVA e o caminho correto.

Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Configurar privilégios sudo para usuários não root para host Linux

O SnapCenter 2.0 e versões posteriores permitem que um usuário não root instale o Pacote de plug-ins do SnapCenter para Linux e inicie o processo de plug-in. Os processos do plug-in serão executados como um usuário não root efetivo. Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se a umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro dela tenham permissão de 555. Caso contrário, a instalação do plug-in poderá falhar.
- Para o usuário não root, certifique-se de que o nome do usuário não root e o nome do grupo do usuário sejam os mesmos.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos do código de autenticação de mensagens: MACs hmac-sha2-256 e MACs hmac-sha2-512.

  Reinicie o serviço sshd após atualizar o arquivo de configuração.

  Exemplo:

```
#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
```

Sobre esta tarefa

Você deve configurar privilégios sudo para que o usuário não root forneça acesso aos seguintes caminhos:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /localização_personalizada/ NetApp/snapcenter/spl/instalação/plugins/desinstalação
- /localização_personalizada/ NetApp/snapcenter/spl/bin/spl

Passos

1. Efetue login no host Linux no qual você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
2. Adicione as seguintes linhas ao arquivo /etc/sudoers usando o utilitário visudo Linux.

```
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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Se você tiver uma configuração RAC, junto com os outros comandos permitidos, você deve adicionar o seguinte ao arquivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Você pode obter o valor de *crs_home* do arquivo */etc/oracle/olr.loc*.

LINUX_USER é o nome do usuário não root que você criou.

Você pode obter o *checksum_value* do arquivo **sc_unix_plugins_checksum.txt**, localizado em:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Linux.

O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Requisitos do host AIX

Você deve garantir que o host atenda aos requisitos antes de instalar o Pacote de plug-ins do SnapCenter para AIX.

O SnapCenter Plug-in para UNIX, que faz parte do Pacote de Plug-ins SnapCenter para AIX, não oferece suporte a grupos de volumes simultâneos.

Item	Requisitos
Sistemas operacionais	AIX 7.1 ou posterior
RAM mínima para o plug-in SnapCenter no host	4 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	2 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.

Item	Requisitos
Pacotes de software necessários	Java 11 IBM Java Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em /var/opt/snapcenter/spl/etc/spl.properties esteja definida para a versão correta do JAVA e o caminho correto.

Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Configurar privilégios sudo para usuários não root para host AIX

O SnapCenter 4.4 e versões posteriores permitem que um usuário não root instale o Pacote de plug-ins do SnapCenter para AIX e inicie o processo de plug-in. Os processos do plug-in serão executados como um usuário não root efetivo. Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se a umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro dela tenham permissão de 555. Caso contrário, a instalação do plug-in poderá falhar.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos do código de autenticação de mensagens: MACs hmac-sha2-256 e MACs hmac-sha2-512.

  Reinicie o serviço sshd após atualizar o arquivo de configuração.

  Exemplo:

```
#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
```

Sobre esta tarefa

Você deve configurar privilégios sudo para que o usuário não root forneça acesso aos seguintes caminhos:

- /home/*AIX_USER*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /localização_personalizada/ NetApp/snapcenter/spl/instalação/plugins/desinstalação
- /localização_personalizada/ NetApp/snapcenter/spl/bin/spl

Passos

1. Efetue login no host AIX no qual você deseja instalar o Pacote de plug-ins do SnapCenter para AIX.
2. Adicione as seguintes linhas ao arquivo /etc/sudoers usando o utilitário visudo Linux.

```
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
```

Se você tiver uma configuração RAC, junto com os outros comandos permitidos, você deve adicionar o seguinte ao arquivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Você pode obter o valor de *crs_home* do arquivo */etc/oracle/olr.loc*.

AIX_USER é o nome do usuário não root que você criou.

Você pode obter o *checksum_value* do arquivo **sc_unix_plugins_checksum.txt**, localizado em:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Linux.

O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Configurar credenciais

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter . Você deve criar credenciais para instalar o pacote de plug-in em hosts Linux ou AIX.

Sobre esta tarefa

As credenciais são criadas para o usuário root ou para um usuário não root que tenha privilégios sudo para instalar e iniciar o processo do plug-in.

Para mais informações, consulte:Configurar privilégios sudo para usuários não root para host Linux ouConfigurar privilégios sudo para usuários não root para host AIX

Melhores práticas: embora você tenha permissão para criar credenciais após implantar hosts e instalar plug-ins, a melhor prática é criar credenciais depois de adicionar SVMs, antes de implantar hosts e instalar plug-ins.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.
4. Na página Credencial, insira as informações da credencial:

Para este campo…	Faça isso…
Nome da credencial	Digite um nome para as credenciais.
Nome de usuário/Senha	Digite o nome de usuário e a senha que serão usados para autenticação. • Administrador de domínio Especifique o administrador de domínio do sistema no qual você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS\Nome do Usuário* ◦ *FQDN do domínio\Nome do usuário* • Administrador local (somente para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é: *UserName*

Para este campo…	Faça isso…
Modo de autenticação	Selecione o modo de autenticação que você deseja usar. Dependendo do sistema operacional do host do plug-in, selecione Linux ou AIX.
Use privilégios sudo	Marque a caixa de seleção **Usar privilégios sudo** se estiver criando credenciais para um usuário não root.

5. Clique em **OK**.

Depois de concluir a configuração das credenciais, talvez você queira atribuir a manutenção de credenciais a um usuário ou grupo de usuários na página **Usuário e acesso**.

Configurar credenciais para um banco de dados Oracle

Você deve configurar credenciais que são usadas para executar operações de proteção de dados em bancos de dados Oracle.

Sobre esta tarefa

Você deve revisar os diferentes métodos de autenticação suportados pelo banco de dados Oracle. Para obter informações, consulte"Métodos de autenticação para suas credenciais" .

Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver privilégios de administrador completos, o nome de usuário deverá ter pelo menos privilégios de grupo de recursos e de backup.

Se você tiver habilitado a autenticação do banco de dados Oracle, um ícone de cadeado vermelho será exibido na exibição de recursos. Você deve configurar as credenciais do banco de dados para poder proteger o banco de dados ou adicioná-lo ao grupo de recursos para executar operações de proteção de dados.

Se você especificar detalhes incorretos ao criar uma credencial, uma mensagem de erro será exibida. Você deve clicar em **Cancelar** e tentar novamente.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** na lista **Exibir**.
3. Clique e selecione o nome do host e o tipo de banco de dados para filtrar os recursos.

   Você pode então clicar para fechar o painel de filtro.

4. Selecione o banco de dados e clique em **Configurações do banco de dados** > **Configurar banco de dados**.
5. Na seção Configurar definições do banco de dados, na lista suspensa **Usar credencial existente**, selecione a credencial que deve ser usada para executar trabalhos de proteção de dados no banco de dados Oracle.

O usuário Oracle deve ter privilégios sysdba.

Você também pode criar uma credencial clicando em + .

6. Na seção Configurar configurações do ASM, na lista suspensa **Usar credencial existente**, selecione a credencial que deve ser usada para executar trabalhos de proteção de dados na instância do ASM.

   O usuário ASM deve ter privilégio sysasm.

   Você também pode criar uma credencial clicando em + .

7. Na seção Configurar definições do catálogo RMAN, na lista suspensa **Usar credencial existente**, selecione a credencial que deve ser usada para executar trabalhos de proteção de dados no banco de dados do catálogo do Oracle Recovery Manager (RMAN).

   Você também pode criar uma credencial clicando em + .

   No campo **TNSName**, insira o nome do arquivo Transparent Network Substrate (TNS) que será usado pelo SnapCenter Server para se comunicar com o banco de dados.

8. No campo **Nós RAC preferenciais**, especifique os nós do Real Application Cluster (RAC) preferidos para backup.

   Os nós preferenciais podem ser um ou todos os nós do cluster onde as instâncias do banco de dados RAC estão presentes. A operação de backup é acionada somente nesses nós preferenciais na ordem de preferência.

   No RAC One Node, apenas um nó é listado nos nós preferenciais, e esse nó preferencial é o nó onde o banco de dados está hospedado atualmente.

   Após o failover ou a realocação do banco de dados do RAC One Node, a atualização dos recursos na página Recursos do SnapCenter removerá o host da lista **Nós RAC Preferenciais** onde o banco de dados estava hospedado anteriormente. O nó RAC onde o banco de dados será realocado será listado em **Nós RAC** e precisará ser configurado manualmente como o nó RAC preferencial.

   Para obter mais informações, consulte "Nós preferenciais na configuração do RAC" .

9. Clique em **OK**.

Adicionar hosts e instalar o pacote de plug-ins para Linux ou AIX usando a GUI

Você pode usar a página Adicionar Host para adicionar hosts e, em seguida, instalar o Pacote de Plug-ins SnapCenter para Linux ou o Pacote de Plug-ins SnapCenter para AIX. Os plug-ins são instalados automaticamente nos hosts remotos.

Sobre esta tarefa

Você pode adicionar um host e instalar pacotes de plug-in para um host individual ou para um cluster. Se você estiver instalando o plug-in em um cluster (Oracle RAC), o plug-in será instalado em todos os nós do cluster. Para o Oracle RAC One Node, você deve instalar o plug-in nos nós ativos e passivos.

Somente a autenticação baseada em senha é suportada quando você instala o plug-in em um Oracle RAC. A autenticação baseada em chave SSH não é suportada.

Você deve receber uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .

Não é possível adicionar um SnapCenter Server como um host de plug-in a outro SnapCenter Server.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Clique em **Adicionar**.
4. Na página Hosts, execute as seguintes ações:

Para este campo…	Faça isso…
Tipo de host	Selecione **Linux** ou **AIX** como o tipo de host. O SnapCenter Server adiciona o host e, em seguida, instala o Plug-in para Oracle Database e o Plug-in para UNIX, caso os plug-ins ainda não estejam instalados no host.
Nome do host	Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o FQDN. Você pode inserir os endereços IP ou FQDN de um dos seguintes: • Host autônomo • Qualquer nó no ambiente Oracle Real Application Clusters (RAC) O VIP do nó ou o IP de digitalização não são suportados Se você estiver adicionando um host usando o SnapCenter e o host fizer parte de um subdomínio, você deverá fornecer o FQDN.

Para este campo…	Faça isso…
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais. Você pode visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou. O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar Host.

5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a serem instalados.
6. (Opcional) Clique em **Mais opções**.

Para este campo…	Faça isso…
Porta	Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.
Caminho de instalação	O caminho padrão é */opt/ NetApp/snapcenter*. Opcionalmente, você pode personalizar o caminho.
Adicionar todos os hosts no Oracle RAC	Marque esta caixa de seleção para adicionar todos os nós do cluster em um Oracle RAC. Em uma configuração Flex ASM, todos os nós, independentemente de serem nós Hub ou Leaf, serão adicionados.

Para este campo…	Faça isso…
Ignorar verificações de pré-instalação opcionais	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.

7. Clique em **Enviar**.

   Se você não tiver marcado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se ele atende aos requisitos para instalar o plug-in.

   O script de pré-verificação não valida o status do firewall da porta do plug-in se ele estiver especificado nas regras de rejeição do firewall.

   Mensagens de erro ou aviso apropriadas serão exibidas se os requisitos mínimos não forem atendidos. Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em *C:\Program Files\ NetApp\ SnapCenter WebApp* para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, deverá atualizar o arquivo em ambos os nós.

8. Verifique a impressão digital e clique em **Confirmar e Enviar**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós do cluster.

   O SnapCenter não suporta o algoritmo ECDSA.

   A verificação de impressão digital é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitore o progresso da instalação.

   Os arquivos de log específicos da instalação estão localizados em */custom_location/snapcenter/logs*.

Resultado

Todos os bancos de dados no host são descobertos automaticamente e exibidos na página Recursos. Se nada for exibido, clique em **Atualizar recursos**.

Monitorar o status da instalação

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento

- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
   a. Clique em **Filtrar**.
   b. Opcional: especifique a data de início e término.
   c. No menu suspenso Tipo, selecione **Instalação de plug-in**.
   d. No menu suspenso Status, selecione o status da instalação.
   e. Clique em **Aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Formas alternativas de instalar o pacote de plug-ins para Linux ou AIX

Você também pode instalar o Pacote de Plug-ins para Linux ou AIX manualmente usando os cmdlets ou CLIs.

Antes de instalar o plug-in manualmente, você deve validar a assinatura do pacote binário usando a chave **snapcenter_public_key.pub** e **snapcenter_linux_host_plugin.bin.sig** localizadas em *C:\ProgramData\ NetApp\ SnapCenter\Package Repository*.

Certifique-se de que o **OpenSSL 1.0.2g** esteja instalado no host onde você deseja instalar o plug-in.

Valide a assinatura do pacote binário executando o comando:

- Para host Linux: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- Para host AIX: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_aix_host_plugin.bsx.sig snapcenter_aix_host_plugin.bsx`

Instalar em vários hosts remotos usando cmdlets

Você deve usar o cmdlet *Install-SmHostPackage* do PowerShell para instalar o Pacote de plug-ins do SnapCenter para Linux ou o Pacote de plug-ins do SnapCenter para AIX em vários hosts.

O que você vai precisar

Você deve estar conectado ao SnapCenter como um usuário de domínio com direitos de administrador local em cada host no qual deseja instalar o pacote de plug-in.

Passos

1. Inicie o PowerShell.
2. No host do SnapCenter Server, estabeleça uma sessão usando o cmdlet *Open-SmConnection* e insira suas credenciais.
3. Instale o pacote de plug-ins SnapCenter para Linux ou o pacote de plug-ins SnapCenter para AIX usando o cmdlet *Install-SmHostPackage* e os parâmetros necessários.

   Você pode usar a opção *-skipprecheck* quando já tiver instalado os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

   > O script de pré-verificação não valida o status do firewall da porta do plug-in se ele estiver especificado nas regras de rejeição do firewall.

4. Insira suas credenciais para instalação remota.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Instalar no host do cluster

Você deve instalar o SnapCenter Plug-ins Package para Linux ou o SnapCenter Plug-ins Package para AIX em ambos os nós do host do cluster.

Cada um dos nós do host do cluster tem dois IPs. Um dos IPs será o IP público dos respectivos nós e o segundo IP será o IP do cluster compartilhado entre os dois nós.

Passos

1. Instale o SnapCenter Plug-ins Package para Linux ou o SnapCenter Plug-ins Package para AIX em ambos os nós do host do cluster.
2. Valide se os valores corretos para os parâmetros SNAPCENTER_SERVER_HOST, SPL_PORT, SNAPCENTER_SERVER_PORT e SPL_ENABLED_PLUGINS estão especificados no arquivo spl.properties localizado em */var/opt/snapcenter/spl/etc/*.

   Se SPL_ENABLED_PLUGINS não estiver especificado em spl.properties, você poderá adicioná-lo e atribuir o valor SCO,SCU.

3. No host do SnapCenter Server, estabeleça uma sessão usando o cmdlet *Open-SmConnection* e insira suas credenciais.
4. Em cada um dos nós, defina os IPs preferenciais do nó usando o comando *Set-PreferredHostIPsInStorageExportPolicy* sccli e os parâmetros necessários.
5. No host do SnapCenter Server, adicione uma entrada para o IP do cluster e o nome DNS correspondente em *C:\Windows\System32\drivers\etc\hosts*.
6. Adicione o nó ao SnapCenter Server usando o cmdlet *Add-SmHost* especificando o IP do cluster para o nome do host.

Descubra o banco de dados Oracle no nó 1 (supondo que o IP do cluster esteja hospedado no nó 1) e crie um backup do banco de dados. Se ocorrer um failover, você poderá usar o backup criado no nó 1 para restaurar o banco de dados no nó 2. Você também pode usar o backup criado no nó 1 para criar um clone no nó 2.

Haverá volumes, diretórios e arquivos de bloqueio obsoletos se o failover ocorrer enquanto qualquer outra operação do SnapCenter estiver em execução.

Instalar pacote de plug-ins para Linux no modo silencioso

Você pode instalar o pacote de plug-ins SnapCenter para Linux no modo silencioso usando a interface de linha de comando (CLI).

O que você vai precisar

- Você deve revisar os pré-requisitos para instalar o pacote de plug-ins.
- Você deve garantir que a variável de ambiente DISPLAY não esteja definida.

  Se a variável de ambiente DISPLAY estiver definida, você deverá executar unset DISPLAY e tentar instalar manualmente o plug-in.

Sobre esta tarefa

Você precisa fornecer as informações de instalação necessárias ao instalar no modo console, enquanto na instalação no modo silencioso você não precisa fornecer nenhuma informação de instalação.

Passos

1. Baixe o pacote de plug-ins do SnapCenter para Linux no local de instalação do SnapCenter Server.

   O caminho de instalação padrão é *C:\ProgramData\ NetApp\ SnapCenter\PackageRepository*. Este caminho pode ser acessado a partir do host onde o SnapCenter Server está instalado.

2. No prompt de comando, navegue até o diretório onde você baixou o arquivo de instalação.
3. Correr

   ```
   ./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. Edite o arquivo spl.properties localizado em */var/opt/snapcenter/spl/etc/* para adicionar SPL_ENABLED_PLUGINS=SCO,SCU e reinicie o serviço SnapCenter Plug-in Loader .

A instalação do pacote de plug-ins registra os plug-ins no host e não no SnapCenter Server. Você deve registrar os plug-ins no SnapCenter Server adicionando o host usando a GUI do SnapCenter ou o cmdlet do PowerShell. Ao adicionar o host, selecione “Nenhum” como credencial. Depois que o host é adicionado, os plug-ins instalados são descobertos automaticamente.

Instalar pacote de plug-ins para AIX no modo silencioso

Você pode instalar o pacote de plug-ins SnapCenter para AIX no modo silencioso usando a interface de linha de comando (CLI).

O que você vai precisar

- Você deve revisar os pré-requisitos para instalar o pacote de plug-ins.

- Você deve garantir que a variável de ambiente DISPLAY não esteja definida.

  Se a variável de ambiente DISPLAY estiver definida, você deverá executar unset DISPLAY e tentar instalar manualmente o plug-in.

Passos

1. Baixe o pacote de plug-ins do SnapCenter para AIX do local de instalação do SnapCenter Server.

   O caminho de instalação padrão é *C:\ProgramData\ NetApp\ SnapCenter\PackageRepository*. Este caminho pode ser acessado a partir do host onde o SnapCenter Server está instalado.

2. No prompt de comando, navegue até o diretório onde você baixou o arquivo de instalação.
3. Correr

   ```
   ./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. Edite o arquivo spl.properties localizado em */var/opt/snapcenter/spl/etc/* para adicionar SPL_ENABLED_PLUGINS=SCO,SCU e reinicie o serviço SnapCenter Plug-in Loader .

> A instalação do pacote de plug-ins registra os plug-ins no host e não no SnapCenter Server. Você deve registrar os plug-ins no SnapCenter Server adicionando o host usando a GUI do SnapCenter ou o cmdlet do PowerShell. Ao adicionar o host, selecione “Nenhum” como credencial. Depois que o host é adicionado, os plug-ins instalados são descobertos automaticamente.

Configurar o serviço SnapCenter Plug-in Loader

O serviço SnapCenter Plug-in Loader carrega o pacote de plug-in para Linux ou AIX para interagir com o SnapCenter Server. O serviço SnapCenter Plug-in Loader é instalado quando você instala o SnapCenter Plug-ins Package para Linux ou o SnapCenter Plug-ins Package para AIX.

Sobre esta tarefa

Após instalar o SnapCenter Plug-ins Package para Linux ou o SnapCenter Plug-ins Package para AIX, o serviço SnapCenter Plug-in Loader é iniciado automaticamente. Se o serviço SnapCenter Plug-in Loader não iniciar automaticamente, você deve:

- Certifique-se de que o diretório onde o plug-in está operando não seja excluído
- Aumentar o espaço de memória alocado à Máquina Virtual Java

O arquivo spl.properties, localizado em */custom_location/ NetApp/snapcenter/spl/etc/*, contém os seguintes parâmetros. Valores padrão são atribuídos a esses parâmetros.

Nome do parâmetro	Descrição
NÍVEL_LOG	Exibe os níveis de log suportados. Os valores possíveis são TRACE, DEBUG, INFO, WARN, ERROR e FATAL.
PROTOCOLO_SPL	Exibe o protocolo suportado pelo SnapCenter Plug-in Loader. Somente o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver faltando.
PROTOCOLO_DO_SERVIDOR_SNAPCENTER	Exibe o protocolo suportado pelo SnapCenter Server. Somente o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver faltando.
PULAR_ATUALIZAÇÃO_JAVAHOME	Por padrão, o serviço SPL detecta o caminho Java e atualiza o parâmetro JAVA_HOME. Portanto, o valor padrão é definido como FALSE. Você pode definir como TRUE se quiser desabilitar o comportamento padrão e corrigir manualmente o caminho Java.
SPL_KEYSTORE_SENHA	Exibe a senha do arquivo keystore. Você só poderá alterar esse valor se alterar a senha ou criar um novo arquivo de keystore.
PORTA SPL	Exibe o número da porta na qual o serviço SnapCenter Plug-in Loader está em execução. Você pode adicionar o valor se o valor padrão estiver faltando. Você não deve alterar o valor após instalar os plug-ins.
SNAPCENTER_SERVER_HOST	Exibe o endereço IP ou nome do host do SnapCenter Server.
CAMINHO_DE_KEYSTORE_SPL	Exibe o caminho absoluto do arquivo keystore.
PORTA_DO_SERVIDOR_SNAPCENTER	Exibe o número da porta na qual o SnapCenter Server está sendo executado.

Nome do parâmetro	Descrição
CONTAGEM_MÁXIMA_DE_LOGS	Exibe o número de arquivos de log do SnapCenter Plug-in Loader que são retidos na pasta */custom_location/snapcenter/spl/logs*. O valor padrão é definido como 5000. Se a contagem for maior que o valor especificado, os últimos 5000 arquivos modificados serão retidos. A verificação do número de arquivos é feita automaticamente a cada 24 horas a partir do momento em que o serviço SnapCenter Plug-in Loader é iniciado. Se você excluir manualmente o arquivo spl.properties, o número de arquivos a serem retidos será definido como 9999.
JAVA_HOME	Exibe o caminho absoluto do diretório do JAVA_HOME que é usado para iniciar o serviço SPL. Este caminho é determinado durante a instalação e como parte do início do SPL.
TAMANHO_MÁXIMO_DE_LOG	Exibe o tamanho máximo do arquivo de log do trabalho. Quando o tamanho máximo é atingido, o arquivo de log é compactado e os logs são gravados no novo arquivo daquele trabalho.
RETER_REGISTROS_DOS_ÚLTIMOS_DIAS	Exibe o número de dias até os quais os logs são retidos.
HABILITAR_VALIDAÇÃO_DE_CERTIFICADO	Exibe verdadeiro quando a validação do certificado CA está habilitada para o host. Você pode habilitar ou desabilitar esse parâmetro editando o spl.properties ou usando a GUI ou o cmdlet do SnapCenter .

Se algum desses parâmetros não estiver atribuído ao valor padrão ou se você quiser atribuir ou alterar o valor, você poderá modificar o arquivo spl.properties. Você também pode verificar o arquivo spl.properties e editá-lo para solucionar quaisquer problemas relacionados aos valores atribuídos aos parâmetros. Depois de modificar o arquivo spl.properties, você deve reiniciar o serviço SnapCenter Plug-in Loader .

Passos

1. Execute uma das seguintes ações, conforme necessário:
   - Inicie o serviço SnapCenter Plug-in Loader :
     - Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl`

`start`

- Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`

◦ Pare o serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
- Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

> Você pode usar a opção -force com o comando stop para interromper o serviço SnapCenter Plug-in Loader à força. No entanto, você deve ter cuidado antes de fazer isso, pois isso também encerra as operações existentes.

◦ Reinicie o serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`

◦ Encontre o status do serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
- Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`

◦ Encontre a alteração no serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
- Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configurar certificado CA com o serviço SnapCenter Plug-in Loader (SPL) no host Linux

Você deve gerenciar a senha do keystore SPL e seu certificado, configurar o certificado CA, configurar certificados raiz ou intermediários para o trust-store SPL e configurar o par de chaves assinadas pela CA para o trust-store SPL com o serviço SnapCenter Plug-in Loader para ativar o certificado digital instalado.

> O SPL usa o arquivo 'keystore.jks', que está localizado em '/var/opt/snapcenter/spl/etc' como seu armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore SPL e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore SPL a partir do arquivo de propriedades SPL.

É o valor correspondente à chave 'SPL_KEYSTORE_PASS'.

2. Alterar a senha do keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Altere a senha de todos os aliases de entradas de chave privada no
keystore para a mesma senha usada para o keystore:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

Atualize o mesmo para a chave SPL_KEYSTORE_PASS no arquivo spl.properties.

3. Reinicie o serviço após alterar a senha.

> A senha para o keystore SPL e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para armazenamento confiável SPL

Você deve configurar os certificados raiz ou intermediários sem a chave privada para o armazenamento confiável SPL.

Passos

1. Navegue até a pasta que contém o keystore SPL: */var/opt/snapcenter/spl/etc*.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

```
 keytool -list -v -keystore keystore.jks
. Adicione um certificado raiz ou intermediário:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Reinicie o serviço após configurar os certificados raiz ou
intermediários para o armazenamento confiável SPL.
```

> Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL

Você deve configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL.

Passos

1. Navegue até a pasta que contém o keystore do SPL /var/opt/snapcenter/spl/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

```
 keytool -list -v -keystore keystore.jks
. Adicione o certificado da CA com chave privada e pública.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Listar os certificados adicionados no keystore.
```

```
 keytool -list -v -keystore keystore.jks
. Verifique se o keystore contém o alias correspondente ao novo
certificado CA, que foi adicionado ao keystore.
. Altere a senha da chave privada adicionada para o certificado CA para
a senha do keystore.
```

A senha padrão do keystore SPL é o valor da chave SPL_KEYSTORE_PASS no arquivo spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Se o nome do alias no certificado da CA for longo e contiver espaços
ou caracteres especiais ("*",","), altere o nome do alias para um nome
simples:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configure o nome do alias do keystore localizado no arquivo
spl.properties.
```

Atualize este valor em relação à chave SPL_CERTIFICATE_ALIAS.

4. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL.

Configurar lista de revogação de certificados (CRL) para SPL

Você deve configurar o CRL para SPL

Sobre esta tarefa

- O SPL procurará os arquivos CRL em um diretório pré-configurado.

- O diretório padrão para os arquivos CRL do SPL é */var/opt/snapcenter/spl/etc/crl*.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo spl.properties com a chave SPL_CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

   Os certificados recebidos serão verificados em relação a cada CRL.

Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *Get-SmCertificateSettings*.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- *  * indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- *  * indica que o certificado CA foi validado com sucesso.
- *  * indica que o certificado CA não pôde ser validado.
- *  * indica que as informações de conexão não puderam ser recuperadas.

Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Importar dados do SnapManager para Oracle e SnapManager para SAP para o SnapCenter

Importar dados do SnapManager para Oracle e SnapManager para SAP para o SnapCenter permite que você continue usando seus dados de versões anteriores.

Você pode importar dados do SnapManager para Oracle e do SnapManager para SAP para o SnapCenter executando a ferramenta de importação na interface de linha de comando (CLI do host Linux).

A ferramenta de importação cria políticas e grupos de recursos no SnapCenter. As políticas e os grupos de recursos criados no SnapCenter correspondem aos perfis e operações executados usando esses perfis no SnapManager para Oracle e no SnapManager para SAP. A ferramenta de importação SnapCenter interage com os bancos de dados de repositório SnapManager para Oracle e SnapManager para SAP e com o banco de dados que você deseja importar.

- Recupera todos os perfis, programações e operações executadas usando os perfis.
- Cria uma política de backup do SnapCenter para cada operação exclusiva e cada agendamento anexado a um perfil.
- Cria um grupo de recursos para cada banco de dados de destino.

Você pode executar a ferramenta de importação executando o script sc-migrate localizado em */opt/ NetApp/snapcenter/spl/bin*. Quando você instala o pacote de plug-ins SnapCenter para Linux no host do banco de dados que deseja importar, o script sc-migrate é copiado para */opt/ NetApp/snapcenter/spl/bin*.

A importação de dados não é suportada pela interface gráfica do usuário (GUI) do SnapCenter .

O SnapCenter não oferece suporte ao Data ONTAP operando no Modo 7. Você pode usar a Ferramenta de Transição de 7 Modos para migrar dados e configurações armazenados em um sistema executando o Data ONTAP operando no Modo 7 para um sistema ONTAP .

Configurações suportadas para importação de dados

Antes de importar dados do SnapManager 3.4.x para Oracle e do SnapManager 3.4.x para SAP para o SnapCenter, você deve estar ciente das configurações suportadas pelo SnapCenter Plug-in para Oracle Database.

As configurações suportadas com o SnapCenter Plug-in para Oracle Database estão listadas no "Ferramenta de Matriz de Interoperabilidade da NetApp" .

O que é importado para o SnapCenter

Você pode importar perfis, programações e operações realizadas usando os perfis.

Do SnapManager para Oracle e SnapManager para SAP	Para SnapCenter
Perfis sem quaisquer operações e horários	Uma política é criada com o tipo de backup padrão como Online e o escopo do backup como Completo.
Perfis com uma ou mais operações	Várias políticas são criadas com base em uma combinação exclusiva de um perfil e operações executadas usando esse perfil. As políticas criadas no SnapCenter contêm os detalhes de poda e retenção do log de arquivamento recuperados do perfil e das operações correspondentes.

Do SnapManager para Oracle e SnapManager para SAP	Para SnapCenter
Perfis com configuração do Oracle Recovery Manager (RMAN)	As políticas são criadas com a opção **Backup de catálogo com Oracle Recovery Manager** habilitada. Se a catalogação RMAN externa foi usada no SnapManager, você deve configurar as definições do catálogo RMAN no SnapCenter. Você pode selecionar a credencial existente ou criar uma nova credencial. Se o RMAN foi configurado por meio do arquivo de controle no SnapManager, você não precisa configurar o RMAN no SnapCenter.
Cronograma anexado a um perfil	Uma política é criada apenas para o cronograma.
Banco de dados	Um grupo de recursos é criado para cada banco de dados importado. Em uma configuração de Real Application Clusters (RAC), o nó no qual você executa a ferramenta de importação se torna o nó preferencial após a importação e o grupo de recursos é criado para esse nó.

Quando um perfil é importado, uma política de verificação é criada junto com a política de backup.

Quando os perfis, programações e quaisquer operações executadas usando os perfis do SnapManager para Oracle e do SnapManager para SAP são importados para o SnapCenter, os diferentes valores de parâmetros também são importados.

Parâmetros e valores do SnapManager para Oracle e SnapManager para SAP	Parâmetros e valores do SnapCenter	Notas
Escopo de backup • Completo • Dados • Registro	Escopo de backup • Completo • Dados • Registro	

Parâmetros e valores do SnapManager para Oracle e SnapManager para SAP	Parâmetros e valores do SnapCenter	Notas
Modo de backup • Auto • On-line • Off-line	Tipo de backup • On-line • Desligamento offline	Se o modo de backup for Automático, a ferramenta de importação verificará o estado do banco de dados quando a operação foi realizada e definirá apropriadamente o tipo de backup como Desligamento Online ou Offline.
Retenção • Dias • Contagens	Retenção • Dias • Contagens	O SnapManager para Oracle e o SnapManager para SAP usam Dias e Contagens para definir a retenção. No SnapCenter, há Dias *OU* Contagens. Portanto, a retenção é definida em relação aos dias, pois os dias têm preferência sobre as contagens no SnapManager para Oracle e no SnapManager para SAP.
Poda para Cronogramas • Todos • número de alteração do sistema (SCN) • Data • Registros criados antes de horas, dias, semanas e meses especificados	Poda para Cronogramas • Todos • Registros criados antes de horas e dias especificados	O SnapCenter não oferece suporte à poda com base em SCN, data, semanas e meses.
Notificação • E-mails enviados apenas para operações bem-sucedidas • E-mails enviados apenas para operações com falha • E-mails enviados para operações bem-sucedidas e malsucedidas	Notificação • Sempre • Em caso de falha • Aviso • Erro	As notificações por e-mail são importadas. No entanto, você deve atualizar manualmente o servidor SMTP usando a GUI do SnapCenter . O assunto do e-mail é deixado em branco para você configurar.

O que não é importado para o SnapCenter

A ferramenta de importação não importa tudo para o SnapCenter.

Você não pode importar o seguinte para o SnapCenter:

- Metadados de backup
- Backups parciais
- Mapeamento de dispositivos brutos (RDM) e backups relacionados ao Virtual Storage Console (VSC)
- Funções ou quaisquer credenciais disponíveis no repositório SnapManager para Oracle e SnapManager para SAP
- Dados relacionados a operações de verificação, restauração e clonagem
- Poda para operações
- Detalhes de replicação especificados no perfil do SnapManager para Oracle e SnapManager para SAP

  Após a importação, você deve editar manualmente a política correspondente criada no SnapCenter para incluir os detalhes de replicação.

- Informações de backup catalogadas

Preparar para importar dados

Antes de importar dados para o SnapCenter, você deve executar determinadas tarefas para executar a operação de importação com sucesso.

Passos

1. Identifique o banco de dados que você deseja importar.
2. Usando o SnapCenter, adicione o host do banco de dados e instale o pacote de plug-ins do SnapCenter para Linux.
3. Usando o SnapCenter, configure as conexões para as máquinas virtuais de armazenamento (SVMs) usadas pelos bancos de dados no host.
4. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
5. Na página Recursos, certifique-se de que o banco de dados a ser importado seja descoberto e exibido.

   Quando você quiser executar a ferramenta de importação, o banco de dados deve estar acessível, caso contrário, a criação do grupo de recursos falhará.

   Se o banco de dados tiver credenciais configuradas, você deverá criar uma credencial correspondente no SnapCenter, atribuir a credencial ao banco de dados e, em seguida, executar novamente a descoberta do banco de dados. Se o banco de dados estiver residindo no Automatic Storage Management (ASM), você deverá criar credenciais para a instância do ASM e atribuir a credencial ao banco de dados.

6. Certifique-se de que o usuário que executa a ferramenta de importação tenha privilégios suficientes para executar comandos CLI do SnapManager for Oracle ou SnapManager for SAP (como o comando para suspender agendamentos) do host do SnapManager for Oracle ou SnapManager for SAP.
7. Execute os seguintes comandos no host SnapManager for Oracle ou SnapManager for SAP para suspender os agendamentos:
   a. Se você quiser suspender os agendamentos no host SnapManager for Oracle, execute:
      - `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`

  Você deve executar o comando smo credential set para cada perfil no host.

b. Se você quiser suspender os agendamentos no host SnapManager para SAP, execute:

- `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`

  Você deve executar o comando smsap credential set para cada perfil no host.

8. Certifique-se de que o nome de domínio totalmente qualificado (FQDN) do host do banco de dados seja exibido quando você executar hostname -f.

   Se o FQDN não for exibido, você deve modificar /etc/hosts para especificar o FQDN do host.

Importar dados

Você pode importar dados executando a ferramenta de importação do host do banco de dados.

Sobre esta tarefa

As políticas de backup do SnapCenter criadas após a importação têm formatos de nomenclatura diferentes:

- As políticas criadas para os perfis sem quaisquer operações e programações têm o formato SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED.

  Quando nenhuma operação é executada usando um perfil, a política correspondente é criada com o tipo de backup padrão como online e o escopo do backup como completo.

- As políticas criadas para os perfis com uma ou mais operações têm o formato SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED.
- As políticas criadas para os agendamentos anexados aos perfis têm o formato SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED.

Passos

1. Efetue login no host do banco de dados que você deseja importar.
2. Execute a ferramenta de importação executando o script sc-migrate localizado em */opt/NetApp/snapcenter/spl/bin*.
3. Digite o nome de usuário e a senha do SnapCenter Server.

Após validar as credenciais, uma conexão é estabelecida com o SnapCenter.

4. Insira os detalhes do banco de dados do repositório SnapManager para Oracle ou SnapManager para SAP.

   O banco de dados do repositório lista os bancos de dados que estão disponíveis no host.

5. Insira os detalhes do banco de dados de destino.

   Se você quiser importar todos os bancos de dados no host, digite all.

6. Se você quiser gerar um log do sistema ou enviar mensagens ASUP para operações com falha, você deve habilitá-los executando o comando *Add-SmStorageConnection* ou *Set-SmStorageConnection*.

> Se desejar cancelar uma operação de importação, durante a execução da ferramenta de importação ou após a importação, você deverá excluir manualmente as políticas, credenciais e grupos de recursos do SnapCenter que foram criados como parte da operação de importação.

Resultados

As políticas de backup do SnapCenter são criadas para perfis, agendamentos e operações executadas usando os perfis. Grupos de recursos também são criados para cada banco de dados de destino.

Após a importação bem-sucedida dos dados, os agendamentos associados ao banco de dados importado são suspensos no SnapManager para Oracle e no SnapManager para SAP.

> Após a importação, você deve gerenciar o banco de dados ou sistema de arquivos importado usando o SnapCenter.

Os logs de cada execução da ferramenta de importação são armazenados no diretório */var/opt/snapcenter/spl/logs* com o nome spl_migration_timestamp.log. Você pode consultar este log para revisar erros de importação e solucioná-los.

Instalar o SnapCenter Plug-in for VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs), ou se você quiser proteger VMs e armazenamentos de dados, será necessário implantar o SnapCenter Plug-in for VMware vSphere .

Para obter informações sobre como implantar, consulte "Visão geral da implantação" .

Implantar certificado CA

Para configurar o Certificado CA com o SnapCenter Plug-in for VMware vSphere, consulte "Criar ou importar certificado SSL" .

Configurar o arquivo CRL

O SnapCenter Plug-in for VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL do SnapCenter Plug-in for VMware vSphere é */opt/netapp/config/crl*.

Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Prepare-se para proteger bancos de dados Oracle

Antes de executar qualquer operação de proteção de dados, como operações de backup, clonagem ou restauração, você deve definir sua estratégia e configurar o ambiente. Você também pode configurar o SnapCenter Server para usar a tecnologia SnapMirror e SnapVault .

Para aproveitar a tecnologia SnapVault e SnapMirror , você deve configurar e inicializar um relacionamento de proteção de dados entre os volumes de origem e destino no dispositivo de armazenamento. Você pode usar o NetAppSystem Manager ou usar a linha de comando do console de armazenamento para executar essas tarefas.

Antes de usar o Plug-in para Oracle Database, o administrador do SnapCenter deve instalar e configurar o SnapCenter Server e executar as tarefas de pré-requisito.

- Instalar e configurar o SnapCenter Server."Saber mais"
- Configure o ambiente SnapCenter adicionando conexões do sistema de armazenamento."Saber mais"

> O SnapCenter não oferece suporte a várias SVMs com o mesmo nome em clusters diferentes. Cada SVM registrado no SnapCenter usando registro de SVM ou registro de cluster deve ser exclusivo.

- Crie credenciais com modo de autenticação como Linux ou AIX para o usuário de instalação."Saber mais"
- Adicione hosts, instale os plug-ins e descubra os recursos.
- Se você estiver usando o SnapCenter Server para proteger bancos de dados Oracle que residem em LUNs ou VMDKs do VMware RDM, será necessário implantar o SnapCenter Plug-in for VMware vSphere e registrar o plug-in no SnapCenter.
- Instale o Java no seu host Linux ou AIX.

  Ver"Requisitos do host Linux" ou"Requisitos do host AIX" para mais informações.

- Você deve definir o valor de tempo limite do firewall do aplicativo para 3 horas ou mais.
- Se você tiver bancos de dados Oracle em ambientes NFS, deverá ter configurado pelo menos um LIF de dados NFS para armazenamento primário ou secundário para executar operações de montagem, clonagem, verificação e restauração.
- Se você tiver vários caminhos de dados (LIFs) ou uma configuração dNFS, poderá executar o seguinte usando a CLI do SnapCenter no host do banco de dados:
  - Por padrão, todos os endereços IP do host do banco de dados são adicionados à política de exportação de armazenamento NFS na máquina virtual de armazenamento (SVM) para os volumes clonados. Se você quiser ter um endereço IP específico ou restringir a um subconjunto de endereços IP, execute a CLI Set-PreferredHostIPsInStorageExportPolicy.
  - Se você tiver vários caminhos de dados (LIFs) no SVM, o SnapCenter escolherá o caminho de dados (LIF) apropriado para montar o volume clonado do NFS. No entanto, se você quiser especificar um caminho de dados específico (LIF), deverá executar a CLI Set-SvmPreferredDataPath. O guia de referência de comandos tem mais informações.

- Se você tiver bancos de dados Oracle em ambientes SAN, certifique-se de que o ambiente SAN esteja configurado conforme a recomendação mencionada nos seguintes guias:
  - "Usando hosts Linux com armazenamento ONTAP"
  - "Configurações do host afetadas pelos utilitários do host AIX"
- Se você tiver bancos de dados Oracle no LVM em sistemas operacionais Oracle Linux ou RHEL, instale a versão mais recente do Logical Volume Management (LVM).
- Se você estiver usando o SnapManager para Oracle e quiser migrar para o SnapCenter Plug-in para Oracle Database, poderá migrar os perfis para políticas e grupos de recursos do SnapCenter usando o comando sccli sc-migrate.
- Configure o SnapMirror e o SnapVault no ONTAP, se desejar replicação de backup

Para usuários do SnapCenter 4.1.1, a documentação do SnapCenter Plug-in for VMware vSphere 4.1.1 contém informações sobre como proteger bancos de dados e sistemas de arquivos virtualizados. Para usuários do SnapCenter 4.2.x, a documentação do NetApp Data Broker 1.0 e 1.0.1 contém informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o SnapCenter Plug-in for VMware vSphere fornecido pelo dispositivo virtual NetApp Data Broker baseado em Linux (formato Open Virtual Appliance). Para usuários do SnapCenter 4.3.x, a documentação do SnapCenter Plug-in for VMware vSphere 4.3 contém informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o dispositivo virtual SnapCenter Plug-in for VMware vSphere baseado em Linux (formato Open Virtual Appliance).

Encontre mais informações

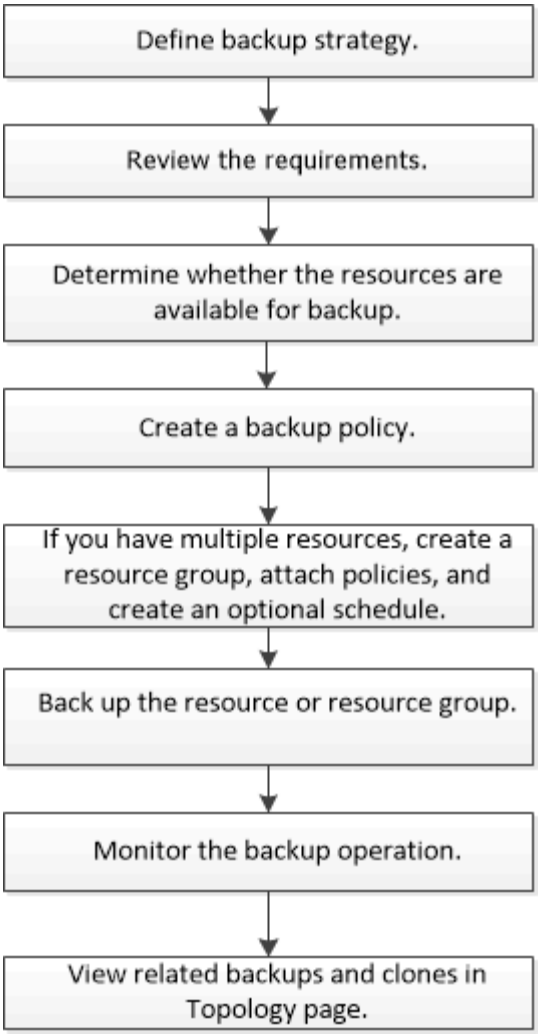
- "Ferramenta de Matriz de Interoperabilidade"
- "Documentação do SnapCenter Plug-in for VMware vSphere"
- "A operação de proteção de dados falha em um ambiente não multicaminho no RHEL 7 e posterior"

Fazer backup de bancos de dados Oracle

Visão geral do procedimento de backup

Você pode criar um backup de um recurso (banco de dados) ou grupo de recursos. O procedimento de backup inclui planejamento, identificação dos recursos para backup, criação de políticas de backup, criação de grupos de recursos e anexação de políticas, criação de backups e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de backup:



Ao criar um backup para bancos de dados Oracle, um arquivo de bloqueio operacional (*.sm_lock_dbsid*) é criado no host do banco de dados Oracle no diretório */var/opt/snapcenter/sco/lock* para evitar que várias operações sejam executadas no banco de dados. Após o backup do banco de dados, o arquivo de bloqueio operacional é removido automaticamente.

Entretanto, se o backup anterior foi concluído com um aviso, o arquivo de bloqueio operacional pode não ser excluído, e a próxima operação de backup entra na fila de espera. Ele pode eventualmente ser cancelado se o arquivo **.sm_lock_dbsid** não for excluído. Nesse cenário, você deve excluir manualmente o arquivo de bloqueio operacional executando as seguintes etapas:

1. No prompt de comando, navegue até */var/opt/snapcenter/sco/lock*.
2. Exclua o bloqueio operacional:`rm -rf .sm_lock_dbsid.`

Informações de configuração de backup

Configurações de banco de dados Oracle suportadas para backups

O SnapCenter suporta backup de diferentes configurações de banco de dados Oracle.

- Oracle autônomo
- Clusters de aplicativos reais Oracle (RAC)

- Oracle Standalone Legacy
- Banco de Dados de Contêineres Autônomos Oracle (CDB)
- Oracle Data Guard em espera

  Você só pode criar backups de montagem offline de bancos de dados standby do Data Guard. Backup com desligamento offline, backup somente de log de arquivo e backup completo não são suportados.

- Oracle Active Data Guard em espera

  Você só pode criar backups on-line de bancos de dados em espera do Active Data Guard. O backup somente do log de arquivo e o backup completo não são suportados.

  Antes de criar um backup do banco de dados Data Guard standby ou Active Data Guard standby, o processo de recuperação gerenciada (MRP) é interrompido e, depois que o backup é criado, o MRP é iniciado.

- Gerenciamento Automático de Armazenamento (ASM)
  - ASM autônomo e ASM RAC em disco de máquina virtual (VMDK)

    Entre todos os métodos de restauração suportados para bancos de dados Oracle, você pode executar somente a restauração de conexão e cópia de bancos de dados ASM RAC no VMDK.

  - ASM autônomo e ASM RAC no mapeamento de dispositivos Raw (RDM) + Você pode executar operações de backup, restauração e clonagem em bancos de dados Oracle no ASM, com ou sem ASMLib.
  - Driver de filtro Oracle ASM (ASMFD)

    As operações de migração e clonagem de PDB não são suportadas.

  - Oracle Flex ASM

Para obter as informações mais recentes sobre as versões Oracle suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Tipos de backup suportados para bancos de dados Oracle

O tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter oferece suporte a tipos de backup online e offline para bancos de dados Oracle.

Backup on-line

Um backup criado quando o banco de dados está no estado online é chamado de backup online. Também chamado de backup dinâmico, um backup on-line permite que você crie um backup do banco de dados sem desligá-lo.

Como parte do backup online, você pode criar um backup dos seguintes arquivos:

- Somente arquivos de dados e arquivos de controle
- Somente arquivos de log de arquivamento (o banco de dados não é colocado no modo de backup neste cenário)
- Banco de dados completo que inclui arquivos de dados, arquivos de controle e arquivos de log de arquivamento

Backup offline

Um backup criado quando o banco de dados está montado ou desligado é chamado de backup offline. Um backup offline também é chamado de backup frio. Você pode incluir apenas arquivos de dados e arquivos de controle em backups offline. Você pode criar um backup de montagem offline ou de desligamento offline.

- Ao criar um backup de montagem offline, você deve garantir que o banco de dados esteja em um estado montado.

  Se o banco de dados estiver em qualquer outro estado, a operação de backup falhará.

- Ao criar um backup de desligamento offline, o banco de dados pode estar em qualquer estado.

  O estado do banco de dados é alterado para o estado necessário para criar um backup. Após criar o backup, o estado do banco de dados é revertido para o estado original.

Como o SnapCenter descobre bancos de dados Oracle

Os recursos são bancos de dados Oracle no host que são mantidos pelo SnapCenter. Você pode adicionar esses bancos de dados a grupos de recursos para executar operações de proteção de dados depois de descobrir os bancos de dados disponíveis.

As seções a seguir descrevem o processo que o SnapCenter usa para descobrir diferentes tipos e versões de bancos de dados Oracle.

Para versões Oracle 11*g* a 12*c*R1

Banco de dados RAC

Os bancos de dados RAC são descobertos apenas com base nas entradas /etc/oratab. Você deve ter as entradas do banco de dados no arquivo /etc/oratab.

Autônomo

Os bancos de dados independentes são descobertos apenas com base nas entradas /etc/oratab.

ASM

A entrada da instância ASM deve estar disponível no arquivo /etc/oratab.

RAC Um Nó

Os bancos de dados do RAC One Node são descobertos apenas com base nas entradas /etc/oratab. Os bancos de dados devem estar no estado nomount, mount ou open. Você deve ter as entradas do banco de dados no arquivo /etc/oratab.

O status do banco de dados do RAC One Node será marcado como renomeado ou excluído se o banco de dados já tiver sido descoberto e houver backups associados ao banco de dados.

Você deve executar as seguintes etapas se o banco de dados for realocado:

1. Adicione manualmente a entrada do banco de dados realocado no arquivo /etc/oratab no nó RAC com failover.
2. Atualize manualmente os recursos.
3. Selecione o banco de dados RAC One Node na página de recursos e clique em Configurações do banco de dados.

4. Configure o banco de dados para definir os nós de cluster preferenciais para o nó RAC que atualmente hospeda o banco de dados.
5. Execute as operações do SnapCenter .
6. Se você tiver realocado um banco de dados de um nó para outro e se a entrada do oratab no nó anterior não for excluída, exclua manualmente a entrada do oratab para evitar que o mesmo banco de dados seja exibido duas vezes.

Para versões Oracle 12cR2 a 18c, 19c ou 21c

Banco de dados RAC

Os bancos de dados RAC são descobertos usando o comando srvctl config. Você deve ter as entradas do banco de dados no arquivo /etc/oratab.

Autônomo

Os bancos de dados independentes são descobertos com base nas entradas no arquivo /etc/oratab e na saída do comando srvctl config.

ASM

A entrada da instância ASM não precisa estar no arquivo /etc/oratab.

RAC Um Nó

Os bancos de dados do RAC One Node são descobertos usando somente o comando srvctl config. Os bancos de dados devem estar no estado nomount, mount ou open. O status do banco de dados do RAC One Node será marcado como renomeado ou excluído se o banco de dados já tiver sido descoberto e houver backups associados ao banco de dados.

Você deve executar as seguintes etapas se o banco de dados for realocado: . Atualize manualmente os recursos. . Selecione o banco de dados RAC One Node na página de recursos e clique em Configurações do banco de dados. . Configure o banco de dados para definir os nós de cluster preferenciais para o nó RAC que atualmente hospeda o banco de dados. . Execute as operações do SnapCenter .

Se houver entradas de banco de dados Oracle 12*c*R2 e 18*c* no arquivo /etc/oratab e o mesmo banco de dados for registrado com o comando srvctl config, o SnapCenter eliminará as entradas duplicadas do banco de dados. Se houver entradas desatualizadas no banco de dados, o banco de dados será descoberto, mas ficará inacessível e o status será offline.

Nós preferenciais na configuração do RAC

Na configuração do Oracle Real Application Clusters (RAC), você pode especificar os nós preferenciais que o SnapCenter usa para executar a operação de backup. Se você não especificar o nó preferencial, o SnapCenter atribuirá automaticamente um nó como o nó preferencial e o backup será criado nesse nó.

Os nós preferenciais podem ser um ou todos os nós do cluster onde as instâncias do banco de dados RAC estão presentes. A operação de backup é acionada somente nesses nós preferenciais na ordem de preferência.

Exemplo

O banco de dados RAC cdbrac tem três instâncias: cdbrac1 no nó 1, cdbrac2 no nó 2 e cdbrac3 no nó 3.

As instâncias node1 e node2 são configuradas para serem os nós preferenciais, com node2 como a primeira

preferência e node1 como a segunda preferência. Quando você executa uma operação de backup, a operação é tentada primeiro no nó2 porque é o primeiro nó preferencial.

Se o node2 não estiver no estado para fazer backup, o que pode ocorrer por vários motivos, como o agente do plug-in não estar em execução no host, a instância do banco de dados no host não estar no estado necessário para o tipo de backup especificado ou a instância do banco de dados no node2 em uma configuração FlexASM não estar sendo atendida pela instância do ASM local; a operação será tentada no node1.

O node3 não será usado para backup porque não está na lista de nós preferenciais.

Configuração do Flex ASM

Em uma configuração do Flex ASM, os nós Leaf não serão listados como nós preferenciais se a cardinalidade for menor que o número de nós no cluster RAC. Se houver alguma alteração nas funções dos nós do cluster Flex ASM, você deverá descobri-las manualmente para que os nós preferenciais sejam atualizados.

Estado do banco de dados necessário

As instâncias do banco de dados RAC nos nós preferenciais devem estar no estado necessário para que o backup seja concluído com sucesso:

- Uma das instâncias do banco de dados RAC nos nós preferenciais configurados deve estar no estado aberto para criar um backup online.
- Uma das instâncias do banco de dados RAC nos nós preferenciais configurados deve estar no estado de montagem, e todas as outras instâncias, incluindo outros nós preferenciais, devem estar no estado de montagem ou inferior para criar um backup de montagem offline.
- As instâncias do banco de dados RAC podem estar em qualquer estado, mas você deve especificar os nós preferenciais para criar um backup de desligamento offline.

Como catalogar backups com o Oracle Recovery Manager

Você pode catalogar os backups de bancos de dados Oracle usando o Oracle Recovery Manager (RMAN) para armazenar as informações de backup no repositório Oracle RMAN.

Os backups catalogados podem ser usados posteriormente para restauração em nível de bloco ou operações de recuperação pontual de tablespace. Quando você não precisar desses backups catalogados, poderá remover as informações do catálogo.

O banco de dados deve estar em estado montado ou superior para catalogação. Você pode executar catalogação em backups de dados, backups de log de arquivo e backups completos. Se a catalogação estiver habilitada para um backup de um grupo de recursos que tenha vários bancos de dados, a catalogação será executada para cada banco de dados. Para bancos de dados Oracle RAC, a catalogação será realizada no nó preferencial onde o banco de dados estiver pelo menos no estado montado.

Se você quiser catalogar backups de um banco de dados RAC, certifique-se de que nenhuma outra tarefa esteja em execução para esse banco de dados. Se outra tarefa estiver em execução, a operação de catalogação falhará em vez de ser enfileirada.

Banco de dados de catálogo externo

Por padrão, o arquivo de controle do banco de dados de destino é usado para catalogação. Se desejar adicionar um banco de dados de catálogo externo, você poderá configurá-lo especificando a credencial e o

nome do Transparent Network Substrate (TNS) do catálogo externo usando o assistente de configurações de banco de dados na interface gráfica do usuário (GUI) do SnapCenter . Você também pode configurar o banco de dados de catálogo externo a partir da CLI executando o comando Configure-SmOracleDatabase com as opções -OracleRmanCatalogCredentialName e -OracleRmanCatalogTnsName.

Comando RMAN

Se você habilitou a opção de catalogação ao criar uma política de backup do Oracle na GUI do SnapCenter , os backups serão catalogados usando o Oracle RMAN como parte da operação de backup. Você também pode executar a catalogação adiada de backups executando o `Catalog-SmBackupWithOracleRMAN` comando.

Após catalogar os backups, você pode executar o `Get-SmBackupDetails` comando para obter as informações de backup catalogadas, como a tag para arquivos de dados catalogados, o caminho do catálogo do arquivo de controle e os locais de log do arquivo catalogado.

Formato de nomenclatura

Se o nome do grupo de discos ASM for maior ou igual a 16 caracteres, a partir do SnapCenter 3.0, o formato de nomenclatura usado para o backup será SC_HASHCODEofDISKGROUP_DBSID_BACKUPID. No entanto, se o nome do grupo de discos tiver menos de 16 caracteres, o formato de nomenclatura usado para o backup será DISKGROUPNAME_DBSID_BACKUPID, que é o mesmo formato usado no SnapCenter 2.0.

O HASHCODEofDISKGROUP é um número gerado automaticamente (2 a 10 dígitos) exclusivo para cada grupo de discos ASM.

Operações de verificação cruzada

Você pode executar verificações cruzadas para atualizar informações desatualizadas do repositório RMAN sobre backups cujos registros de repositório não correspondem ao seu status físico. Por exemplo, se um usuário remover logs arquivados do disco com um comando do sistema operacional, o arquivo de controle ainda indicará que os logs estão no disco, quando na verdade não estão.

A operação de verificação cruzada permite que você atualize o arquivo de controle com as informações. Você pode habilitar a verificação cruzada executando o comando Set-SmConfigSettings e atribuindo o valor TRUE ao parâmetro ENABLE_CROSSCHECK. O valor padrão é definido como FALSO.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

Remover informações do catálogo

Você pode remover as informações do catálogo executando o comando Uncatalog-SmBackupWithOracleRMAN. Não é possível remover as informações do catálogo usando a GUI do SnapCenter . No entanto, as informações de um backup catalogado são removidas durante a exclusão do backup ou durante a exclusão do grupo de retenção e recursos associado a esse backup catalogado.

> Quando você força a exclusão do host SnapCenter , as informações dos backups catalogados associados a esse host não são removidas. Você deve remover informações de todos os backups catalogados para esse host antes de forçar a exclusão do host.

Se a catalogação e a descatalogação falharem porque o tempo de operação excedeu o valor de tempo limite especificado para o parâmetro ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT, você deverá modificar o valor do parâmetro executando o seguinte comando:

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType
Plugin -PluginCode SCO-ConfigSettings
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

Após modificar o valor do parâmetro, reinicie o serviço SnapCenter Plug-in Loader (SPL) executando o seguinte comando:

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando Get-Help command_name. Alternativamente, você pode consultar o "Guia de referência de comandos do software SnapCenter" .

Variáveis de ambiente predefinidas para prescript e postscript específicos de backup

O SnapCenter permite que você use as variáveis de ambiente predefinidas ao executar o prescript e o postscript ao criar políticas de backup. Essa funcionalidade é suportada por todas as configurações do Oracle, exceto VMDK.

O SnapCenter predefine os valores dos parâmetros que serão diretamente acessíveis no ambiente onde os scripts de shell são executados. Você não precisa especificar manualmente os valores desses parâmetros ao executar os scripts.

Variáveis de ambiente predefinidas com suporte para criação de política de backup

- **SC_JOB_ID** especifica o ID do trabalho da operação.

  Exemplo: 256

- **SC_ORACLE_SID** especifica o identificador do sistema do banco de dados.

  Se a operação envolver vários bancos de dados, o parâmetro conterá nomes de bancos de dados separados por barra vertical.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplo: NFSB32|NFSB31

- **SC_HOST** especifica o nome do host do banco de dados.

  Para RAC, o nome do host será o nome do host no qual o backup será executado.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplo: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** especifica o proprietário do sistema operacional do banco de dados.

  Os dados serão formatados como <db1>@<osuser1>|<db2>@<osuser2>.

  Exemplo: NFSB31@oracle|NFSB32@oracle

- **SC_OS_GROUP** especifica o grupo de sistema operacional do banco de dados.

  Os dados serão formatados como <db1>@<osgroup1>|<db2>@<osgroup2>.

Exemplo: NFSB31@install|NFSB32@oinstall

- **SC_BACKUP_TYPE**" especifica o tipo de backup (completo on-line, dados on-line, log on-line, desligamento off-line, montagem off-line)

  Exemplos:

  - Para backup completo: ONLINEFULL
  - backup somente de dados: ONLINEDATA
  - Para backup somente de log: ONLINELOG
- **SC_BACKUP_NAME** especifica o nome do backup.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplo: 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** especifica o ID do backup.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplo: DADOS@203|LOG@205|AV@207
- **SC_ORACLE_HOME** especifica o caminho do diretório inicial do Oracle.

  Exemplo: NFSB32@/ora01/app/oracle/product/18.1.0/db_1|NFSB31@/ora01/app/oracle/product/18.1.0/db_1
- **SC_BACKUP_RETENTION** especifica o período de retenção definido na política.

  Exemplos:

  - Para backup completo: De hora em hora|DADOS@DIAS:3|LOG@CONTAGEM:4
  - Para backup de dados somente sob demanda: Ondemand|DATA@COUNT:2
  - Para backup somente de log sob demanda: Ondemand|LOG@COUNT:2
- **SC_RESOURCE_GROUP_NAME** especifica o nome do grupo de recursos.

  Exemplo: RG1
- **SC_BACKUP_POLICY_NAME** especifica o nome da política de backup.

  Exemplo: backup_policy
- **SC_AV_NAME** especifica os nomes dos volumes do aplicativo.

  Exemplo: AV1|AV2
- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** especifica o mapeamento de armazenamento do SVM para o volume do diretório de arquivos de dados. Será o nome do volume pai para luns e qtrees.

  Os dados serão formatados como <db1>@<SVM1:volume1>|<db2>@<SVM2:volume2>.

Exemplos:

- Para 2 bancos de dados no mesmo grupo de recursos: NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA
- Para um único banco de dados com arquivos de dados distribuídos em vários volumes: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_NFS

- **SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH** especifica o mapeamento de armazenamento do SVM para o volume do diretório de arquivos de logs. Será o nome do volume pai para luns e qtrees.

  Exemplos:

  - Para instância de banco de dados única: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
  - Para múltiplas instâncias de banco de dados: NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO|NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO
- **SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG** especifica a lista de Snapshots contendo o nome do sistema de armazenamento e o nome do volume.

  Exemplos:

  - Para instância de banco de dados única: 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
  - Para várias instâncias de banco de dados: 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** especifica os nomes dos Snapshots primários criados durante o backup.

  Exemplos:

  - Para instância de banco de dados única: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
  - Para várias instâncias de banco de dados: 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
  - Para instantâneos de grupo de consistência que envolvem 2 volumes: 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** especifica os detalhes do ponto de montagem que fazem parte do backup.

  Os detalhes incluem o diretório no qual os volumes são montados e não o pai imediato do arquivo sob backup. Para uma configuração ASM, é o nome do grupo de discos.

Os dados serão formatados como <db1>@<mountpoint1,mountpoint2>|<db2>@<mountpoint1,mountpoint2>.

Exemplos:

- Para instância de banco de dados única: /mnt/nfsdb3_data,/mnt/nfsdb3_log,/mnt/nfsdb3_data1
- Para várias instâncias de banco de dados: NFSB31@/mnt/nfsdb31_data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1|NFSB32@/mnt/nfsdb32_data,/mnt/nfsdb32_log,/mnt/nfsdb32_data1
- Para ASM: +DATA2DG,+LOG2DG

- **SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS** especifica os nomes dos snapshots criados durante o backup de cada um dos pontos de montagem.

  Exemplos:

  - Para instância de banco de dados única: 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
  - Para múltiplas instâncias de banco de dados: 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** especifica o local do diretório de logs de arquivamento.

  Os nomes dos diretórios serão os pais imediatos dos arquivos de log de arquivamento. Se os logs de arquivamento forem colocados em mais de um local, todos os locais serão capturados. Isso também inclui os cenários FRA. Se softlinks forem usados para o diretório, o mesmo será preenchido.

  Exemplos:

  - Para banco de dados único no NFS: /mnt/nfsdb2_log
  - Para vários bancos de dados no NFS e para os logs de arquivamento do banco de dados NFSB31 que são colocados em dois locais diferentes: NFSB31@/mnt/nfsdb31_log1,/mnt/nfsdb31_log2|NFSB32@/mnt/nfsdb32_log
  - Para ASM: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15
- **SC_REDO_LOGS_LOCATIONS** especifica o local do diretório de logs de refazer.

  Os nomes dos diretórios serão o pai imediato dos arquivos de log de refazer. Se softlinks forem usados para o diretório, o mesmo será preenchido.

  Exemplos:

  - Para banco de dados único no NFS: /mnt/nfsdb2_data/newdb1
  - Para vários bancos de dados no NFS: NFSB31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32
  - Para ASM: +LOG2DG/ASMDB2/ONLINELOG
- **SC_CONTROL_FILES_LOCATIONS** especifica o local do diretório dos arquivos de controle.

  Os nomes dos diretórios serão os pais imediatos dos arquivos de controle. Se softlinks forem usados para

o diretório, o mesmo será preenchido.

Exemplos:

- Para banco de dados único no NFS: /mnt/nfsdb2_data/fra/newdb1,/mnt/nfsdb2_data/newdb1
- Para vários bancos de dados no NFS: NFSB31@/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/fra/newdb32,/mnt/nfsdb32_data/newdb32
- Para ASM: +LOG2DG/ASMDB2/CONTROLFILE

- **SC_DATA_FILES_LOCATIONS"** especifica o local do diretório dos arquivos de dados.

  Os nomes dos diretórios serão os pais imediatos dos arquivos de dados. Se softlinks forem usados para o diretório, o mesmo será preenchido.

  Exemplos:

  - Para banco de dados único no NFS: /mnt/nfsdb3_data1,/mnt/nfsdb3_data/NEWDB3/datafile
  - Para vários bancos de dados no NFS: NFSB31@/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/datafile|NFSB32@/mnt/nfsdb32_data1,/mnt/nfsdb32_data/NEWDB32/datafile
  - Para ASM: +DATA2DG/ASMDB2/DATAFILE,+DATA2DG/ASMDB2/TEMPFILE
- **SC_SNAPSHOT_LABEL** especifica o nome dos rótulos secundários.

  Exemplos: por hora, diariamente, semanalmente, mensalmente ou rótulo personalizado.

Delimitadores suportados

- **:** é usado para separar o nome do SVM e o nome do volume

  Exemplo: 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

- **@** é usado para separar dados do nome do banco de dados e para separar o valor da sua chave.

  Exemplos:

  - 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
- **|** é usado para separar os dados entre dois bancos de dados diferentes e para separar os dados entre duas entidades diferentes para os parâmetros SC_BACKUP_ID, SC_BACKUP_RETENTION e SC_BACKUP_NAME.

  Exemplos:

  - DADOS@203|LOG@205

    - Por hora|DADOS@DIAS:3|LOG@CONTAGEM:4
    - DADOS@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- **/** é usado para separar o nome do volume do seu Snapshot para os parâmetros SC_PRIMARY_SNAPSHOT_NAMES e SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG.

  Exemplo: 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

- **,** é usado para separar conjuntos de variáveis para o mesmo banco de dados.

  Exemplo: 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

Opções de retenção de backup

Você pode escolher o número de dias pelos quais deseja manter cópias de backup ou especificar o número de cópias de backup que deseja manter, até um máximo ONTAP de 255 cópias. Por exemplo, sua organização pode exigir que você mantenha 10 dias de cópias de backup ou 130 cópias de backup.

Ao criar uma política, você pode especificar as opções de retenção para o tipo de backup e o tipo de agendamento.

Se você configurar a replicação do SnapMirror , a política de retenção será espelhada no volume de destino.

O SnapCenter exclui os backups retidos que têm rótulos de retenção que correspondem ao tipo de agendamento. Se o tipo de agendamento foi alterado para o recurso ou grupo de recursos, os backups com o rótulo de tipo de agendamento antigo ainda poderão permanecer no sistema.

Para retenção de cópias de backup a longo prazo, você deve usar o backup SnapVault .

Agendamentos de backup

A frequência de backup (tipo de agendamento) é especificada nas políticas; um agendamento de backup é especificado na configuração do grupo de recursos. O fator mais crítico na determinação da frequência ou programação de backup é a taxa de alteração do recurso e a importância dos dados. Você pode fazer backup de um recurso muito utilizado a cada hora, enquanto pode fazer backup de um recurso raramente utilizado uma vez por dia. Outros fatores incluem a importância do recurso para sua organização, seu Acordo de Nível de Serviço (SLA) e seu Objetivo de Ponto de Recuperação (RPO).

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. Um RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. O SLA e o RPO contribuem para a estratégia de proteção de dados.

Mesmo para um recurso muito utilizado, não há necessidade de executar um backup completo mais de uma ou duas vezes por dia. Por exemplo, backups regulares do log de transações podem ser suficientes para garantir que você tenha os backups necessários. Quanto mais você fizer backup dos seus bancos de dados, menos logs de transações o SnapCenter terá que usar no momento da restauração, o que pode resultar em operações de restauração mais rápidas.

Os agendamentos de backup têm duas partes, conforme a seguir:

- Frequência de backup

  A frequência de backup (com que frequência os backups devem ser realizados), chamada de *tipo de agendamento* para alguns plug-ins, faz parte de uma configuração de política. Você pode selecionar por hora, dia, semana ou mês como a frequência de backup da política. Se você não selecionar nenhuma dessas frequências, a política criada será somente sob demanda. Você pode acessar as políticas clicando em **Configurações** > **Políticas**.

- Agendamentos de backup

  Os agendamentos de backup (exatamente quando os backups devem ser executados) fazem parte de uma configuração de grupo de recursos. Por exemplo, se você tiver um grupo de recursos com uma política configurada para backups semanais, poderá configurar o agendamento para fazer backup toda quinta-feira às 22h. Você pode acessar as programações dos grupos de recursos clicando em **Recursos** > **Grupos de Recursos**.

Convenções de nomenclatura de backup

Você pode usar a convenção de nomenclatura padrão do Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um registro de data e hora aos nomes de instantâneos que ajuda a identificar quando as cópias foram criadas.

O Snapshot usa a seguinte convenção de nomenclatura padrão:

```
resourcegroupname_hostname_timestamp
```

Você deve nomear seus grupos de recursos de backup logicamente, como no exemplo a seguir:

```
dts1_mach1x88_03-12-2015_23.17.26
```

Neste exemplo, os elementos de sintaxe têm os seguintes significados:

- *dts1* é o nome do grupo de recursos.
- *mach1x88* é o nome do host.
- *03-12-2015_23.17.26* é a data e o registro de data e hora.

Como alternativa, você pode especificar o formato do nome do Snapshot ao proteger recursos ou grupos de

recursos selecionando **Usar formato de nome personalizado para cópia do Snapshot**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do registro de data e hora é adicionado ao nome do Snapshot.

Requisitos para fazer backup de um banco de dados Oracle

Antes de fazer backup de um banco de dados Oracle, você deve garantir que os pré-requisitos sejam atendidos.

- Você deve ter criado um grupo de recursos com uma política anexada.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.
- Você deve ter atribuído o agregado que está sendo usado pela operação de backup à máquina virtual de armazenamento (SVM) usada pelo banco de dados.
- Você deve ter verificado se todos os volumes de dados e volumes de log de arquivamento pertencentes ao banco de dados estão protegidos se a proteção secundária estiver habilitada para esse banco de dados.
- Você deve ter verificado se o banco de dados que contém arquivos nos grupos de discos ASM deve estar no estado “MOUNT” ou "OPEN`" para verificar seus backups usando o utilitário Oracle DBVERIFY.
- Você deve ter verificado se o comprimento do ponto de montagem do volume não excede 240 caracteres.
- Você deve aumentar o valor de RESTTimeout para 86400000 ms no arquivo *C:\Program Files\ NetApp \SMCore\SMCoreServiceHost.exe.config* no host do SnapCenter Server, se o banco de dados que está sendo feito backup for grande (tamanho em TBs).

  Ao modificar os valores, certifique-se de que não haja trabalhos em execução e reinicie o serviço SnapCenter SMCore após aumentar o valor.

Descubra os bancos de dados Oracle disponíveis para backup

Os recursos são bancos de dados Oracle no host que são gerenciados pelo SnapCenter. Você pode adicionar esses bancos de dados a grupos de recursos para executar operações de proteção de dados depois de descobrir os bancos de dados disponíveis.

Antes de começar

- Você deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts, criar conexões do sistema de armazenamento e adicionar credenciais.
- Se os bancos de dados residirem em um disco de máquina virtual (VMDK) ou mapeamento de dispositivo bruto (RDM), você deverá implantar o SnapCenter Plug-in for VMware vSphere e registrar o plug-in com o SnapCenter.

  Para obter mais informações, consulte "Implantar o SnapCenter Plug-in for VMware vSphere" .
- Se os bancos de dados residirem em um sistema de arquivos VMDK, você deverá ter efetuado login no vCenter e navegado até **Opções da VM** > **Avançado** > **Editar configuração** para definir o valor de *disk.enableUUID* como verdadeiro para a VM.
- Você deve ter revisado o processo que o SnapCenter segue para descobrir diferentes tipos e versões de bancos de dados Oracle.

Etapa 1: impedir que o SnapCenter descubra entradas que não sejam do banco de dados

Você pode impedir que o SnapCenter descubra entradas não pertencentes ao banco de dados adicionadas no arquivo oratab.

Passos

1. Após instalar o plug-in para Oracle, o usuário root deve criar o arquivo **sc_oratab.config** no diretório */var/opt/snapcenter/sco/etc/*.

   Conceda permissão de gravação ao proprietário e ao grupo binário do Oracle para que o arquivo possa ser mantido no futuro.

2. O administrador do banco de dados deve adicionar as entradas que não são do banco de dados no arquivo **sc_oratab.config**.

   É recomendável manter o mesmo formato definido para as entradas não pertencentes ao banco de dados no arquivo */etc/oratab* ou o usuário pode simplesmente adicionar a string de entidade não pertencente ao banco de dados.

   A sequência diferencia maiúsculas de minúsculas. Qualquer texto com # no início é tratado como um comentário. O comentário pode ser anexado após o nome que não seja do banco de dados.

   ```
   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. Descubra os recursos.

   As entradas não pertencentes ao banco de dados adicionadas no **sc_oratab.config** não serão listadas na página Recursos.

   É sempre recomendável fazer um backup do arquivo sc_oratab.config antes de atualizar o plug-in SnapCenter .

Etapa 2: Descubra recursos

Após instalar o plug-in, todos os bancos de dados naquele host são descobertos automaticamente e exibidos na página Recursos.

Os bancos de dados devem estar pelo menos no estado montado ou superior para que a descoberta dos bancos de dados seja bem-sucedida. Em um ambiente Oracle Real Application Clusters (RAC), a instância do banco de dados RAC no host onde a descoberta é realizada deve estar pelo menos no estado montado ou

superior para que a descoberta da instância do banco de dados seja bem-sucedida. Somente os bancos de dados descobertos com sucesso podem ser adicionados aos grupos de recursos.

Se você tiver excluído um banco de dados Oracle no host, o SnapCenter Server não saberá e listará o banco de dados excluído. Você deve atualizar manualmente os recursos para atualizar a lista de recursos do SnapCenter .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** na lista **Exibir**.

   Clique  ícone do filtro] e selecione o nome do host e o tipo de banco de dados para filtrar os recursos. Você pode então clicar no ícone imagfilter_icon.gif[ícone de filtro]_icon.png[] para fechar o painel de filtro.

3. Clique em **Atualizar recursos**.

   Em um cenário RAC One Node, o banco de dados é descoberto como o banco de dados RAC no nó onde ele está hospedado atualmente.

Resultados

Os bancos de dados são exibidos junto com informações como tipo de banco de dados, nome do host ou cluster, grupos de recursos e políticas associados e status.

Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

- Se o banco de dados estiver em um sistema de armazenamento não NetApp , a interface do usuário exibirá uma mensagem Não disponível para backup na coluna Status geral.

  Você não pode executar operações de proteção de dados no banco de dados que está em um sistema de armazenamento não NetApp .

- Se o banco de dados estiver em um sistema de armazenamento NetApp e não estiver protegido, a interface do usuário exibirá uma mensagem Não protegido na coluna Status geral.
- Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, a interface do usuário exibirá uma mensagem Disponível para backup na coluna Status geral.

Se você tiver habilitado uma autenticação de banco de dados Oracle, um ícone de cadeado vermelho será exibido na exibição de recursos. Você deve configurar as credenciais do banco de dados para poder proteger o banco de dados ou adicioná-lo ao grupo de recursos para executar operações de proteção de dados.

Crie políticas de backup para bancos de dados Oracle

Antes de usar o SnapCenter para fazer backup de recursos do banco de dados Oracle, você deve criar uma política de backup para o recurso ou grupo de recursos do qual deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e mantém backups. Você também pode especificar as configurações de replicação, script e tipo de backup. Criar uma política economiza tempo quando você deseja reutilizá-la em outro recurso ou grupo de recursos.

Antes de começar

- Você deve ter definido sua estratégia de backup.
- Você deve estar preparado para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, descobrir bancos de dados e criar conexões de sistema de armazenamento.
- Se você estiver replicando Snapshots para um espelho ou armazenamento secundário de cofre, o administrador do SnapCenter deverá ter atribuído as SVMs a você para os volumes de origem e destino.
- Se você instalou o plug-in como um usuário não root, deverá atribuir manualmente as permissões de execução aos diretórios prescript e postscript.
- Revise os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror . Para obter informações, consulte "Limites de objetos para sincronização ativa do SnapMirror" .

Sobre esta tarefa

Se a opção 'Manter as cópias de backup por um número específico de dias' for selecionada, o período de retenção do SnapLock deverá ser menor ou igual aos dias de retenção mencionados.

+ Especificar um período de bloqueio de Snapshot impede a exclusão dos Snapshots até que o período de retenção expire. Isso pode levar à retenção de um número maior de Snapshots do que a contagem especificada na política.

+ Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos Snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Selecione **Oracle Database** na lista suspensa.
4. Clique em **Novo**.
5. Na página Nome, insira o nome e os detalhes da política.
6. Na página Tipo de política, execute as seguintes etapas:

    a. Selecione seu tipo de armazenamento.

    b. Selecione o escopo da política:

        - Se você quiser **criar um backup on-line**, selecione **Backup on-line**.

          Você deve especificar se deseja fazer backup de todos os arquivos de dados, arquivos de controle e arquivos de log de arquivamento, somente dos arquivos de dados e arquivos de controle ou somente dos arquivos de log de arquivamento.

        - Se você quiser **criar um backup offline**, selecione **Backup offline** e, em seguida, selecione uma das seguintes opções:
            - Se você quiser criar um backup offline quando o banco de dados estiver no estado montado, selecione **Montar**.
            - Se você quiser criar um backup de desligamento offline alterando o banco de dados para o estado de desligamento, selecione **Desligar**.

              Se você tiver bancos de dados plugáveis (PDBs) e quiser salvar o estado dos PDBs antes de

criar o backup, selecione **Salvar estado dos PDBs**. Isso permite que você traga os PDBs ao seu estado original após a criação do backup.

c. Se você quiser catalogar o backup usando o Oracle Recovery Manager (RMAN), selecione **Catalogar backup com o Oracle Recovery Manager (RMAN)**.

   Você pode executar a catalogação adiada para um backup por vez usando a GUI ou o comando SnapCenter CLI Catalog-SmBackupWithOracleRMAN.

   Se você quiser catalogar backups de um banco de dados RAC, certifique-se de que nenhuma outra tarefa esteja em execução para esse banco de dados. Se outra tarefa estiver em execução, a operação de catalogação falhará em vez de ser enfileirada.

d. Se você quiser remover logs de arquivo após o backup, selecione **Remover logs de arquivo após o backup**.

   A remoção de logs de arquivo do destino de log de arquivo que não está configurado no banco de dados será ignorada.

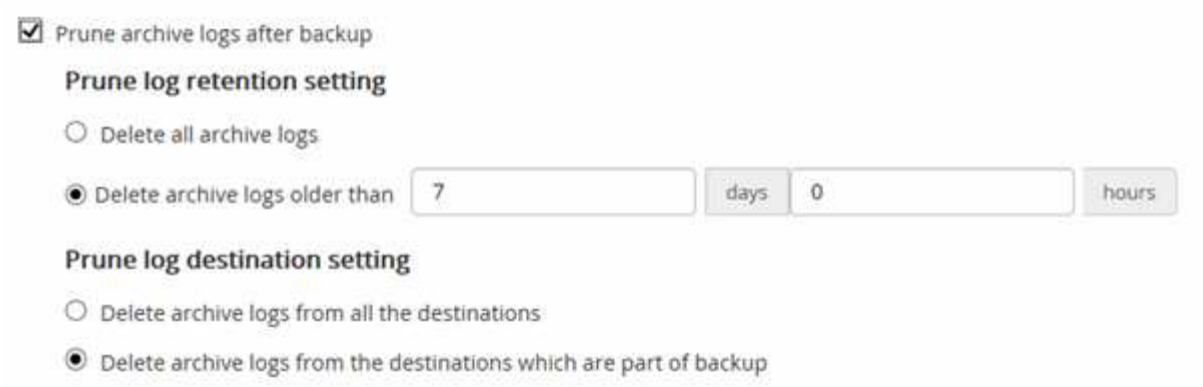
   Se estiver usando o Oracle Standard Edition, você poderá usar os parâmetros LOG_ARCHIVE_DEST e LOG_ARCHIVE_DUPLEX_DEST ao executar o backup do log de arquivamento.

   - Você pode excluir logs de arquivamento somente se tiver selecionado os arquivos de log de arquivamento como parte do seu backup.

     Você deve garantir que todos os nós em um ambiente RAC possam acessar todos os locais de log de arquivamento para que a operação de exclusão seja bem-sucedida.

Se você quiser…	**Então…**
Excluir todos os logs de arquivo	Selecione **Excluir todos os logs de arquivo**.
Excluir logs de arquivo mais antigos	Selecione **Excluir logs de arquivo mais antigos que** e especifique a idade dos logs de arquivo que devem ser excluídos em dias e horas.
Excluir logs de arquivo de todos os destinos	Selecione **Excluir logs de arquivo de todos os destinos**.
Excluir os logs de arquivamento dos destinos de log que fazem parte do backup	Selecione **Excluir logs de arquivo dos destinos que fazem parte do backup**.

+



7. Na página Snapshot e Replicação, execute as seguintes etapas:

   a. Especifique a frequência da programação selecionando **Sob demanda**, **Por hora**, **Diariamente**, **Semanalmente** ou **Mensalmente**.

   Você pode especificar o agendamento (data de início e data de término) para a operação de backup ao criar um grupo de recursos. Isso permite que você crie grupos de recursos que compartilham a mesma política e frequência de backup, mas permite que você atribua agendamentos de backup diferentes a cada política.

   Se você agendou para 2h00, a programação não será acionada durante o horário de verão (DST).

   a. Na seção Configurações de retenção de instantâneo de dados, especifique as configurações de retenção para o tipo de backup e o tipo de agendamento selecionado na página Tipo de backup:

Se você quiser…	Então…

Mantenha um certo número de Snapshots	Selecione **Cópias a serem mantidas** e especifique o número de Snapshots que você deseja manter. Se o número de Snapshots exceder o número especificado, os Snapshots serão excluídos, com as cópias mais antigas sendo excluídas primeiro. O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida como um valor maior do que o suportado pela versão subjacente do ONTAP . Você deve definir a contagem de retenção como 2 ou mais se planeja habilitar a replicação do SnapVault . Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro Snapshot será o Snapshot de referência para o relacionamento SnapVault até que um Snapshot mais recente seja replicado para o destino.
Mantenha os Snapshots por um certo número de dias	Selecione **Manter cópias por** e especifique o número de dias pelos quais você deseja manter os Snapshots antes de excluí-los.
Período de bloqueio de cópia de instantâneo	Selecione o **Período de bloqueio de cópia de instantâneo** e especifique a duração em dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

b. Na seção Configurações de retenção de instantâneo do Archive Log, especifique as configurações de retenção para o tipo de backup e o tipo de agendamento selecionado na página Tipo de backup:

Se você quiser…	Então…

Mantenha um certo número de Snapshots	Selecione **Cópias a serem mantidas** e especifique o número de Snapshots que você deseja manter. Se o número de Snapshots exceder o número especificado, os Snapshots serão excluídos, com as cópias mais antigas sendo excluídas primeiro. O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida como um valor maior do que o suportado pela versão subjacente do ONTAP . Você deve definir a contagem de retenção como 2 ou mais se planeja habilitar a replicação do SnapVault . Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro Snapshot será o Snapshot de referência para o relacionamento SnapVault até que um Snapshot mais recente seja replicado para o destino.
Mantenha os Snapshots por um certo número de dias	Selecione **Manter cópias por** e especifique o número de dias pelos quais você deseja manter os Snapshots antes de excluí-los.
Período de bloqueio de cópia de instantâneo	Selecione o **Período de bloqueio de cópia de instantâneo** e especifique a duração em dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

c. Selecione o rótulo da política.

Você pode atribuir rótulos SnapMirror a snapshots primários para replicação remota, permitindo que os snapshots primários descarreguem a operação de replicação de snapshots do SnapCenter para sistemas secundários ONTAP . Isso pode ser feito sem habilitar a opção SnapMirror ou SnapVault na página de política.

8. Na seção Selecionar opções de replicação secundária, selecione uma ou ambas as seguintes opções de replicação secundária:

Você deve selecionar as opções de replicação secundária para que o **Período de bloqueio de cópia de instantâneo secundário** seja efetivo.

Para este campo…	Faça isso…
Atualizar o SnapMirror após criar um Snapshot local	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Esta opção deve ser habilitada para sincronização ativa do SnapMirror . Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP.
Atualizar o SnapVault após criar um Snapshot local	Selecione esta opção para executar a replicação de backup de disco para disco (backups do SnapVault). Quando o SnapLock é configurado somente no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página Topologia atualiza o período de bloqueio no secundário recuperado do ONTAP. Para mais informações sobre o SnapLock Vault, consulte "Enviar cópias do Snapshot para o WORM em um destino de cofre" Ver "Visualize backups e clones do banco de dados Oracle na página Topologia" .
Contagem de novas tentativas de erro	Insira o número máximo de tentativas de replicação que podem ser permitidas antes que a operação seja interrompida.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o armazenamento secundário para evitar atingir o limite máximo de Snapshots no armazenamento secundário.

9. Na página Script, insira o caminho e os argumentos do prescript ou postscript que você deseja executar antes ou depois da operação de backup, respectivamente.

   Você deve armazenar os prescrições e pós-escritos em */var/opt/snapcenter/spl/scripts* ou em qualquer pasta dentro deste caminho. Por padrão, o caminho */var/opt/snapcenter/spl/scripts* é preenchido. Se você criou alguma pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

   Você também pode especificar o valor do tempo limite do script. O valor padrão é 60 segundos.

O SnapCenter permite que você use as variáveis de ambiente predefinidas ao executar o prescript e o postscript."Saber mais"

10. Na página Verificação, execute as seguintes etapas:

    a. Selecione o agendamento de backup para o qual você deseja executar a operação de verificação.

    b. Na seção Comandos do script de verificação, insira o caminho e os argumentos do prescript ou postscript que você deseja executar antes ou depois da operação de verificação, respectivamente.

       Você deve armazenar os prescrições e pós-escritos em */var/opt/snapcenter/spl/scripts* ou em qualquer pasta dentro deste caminho. Por padrão, o caminho */var/opt/snapcenter/spl/scripts* é preenchido. Se você criou alguma pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

    Você também pode especificar o valor do tempo limite do script. O valor padrão é 60 segundos.

11. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas para bancos de dados Oracle

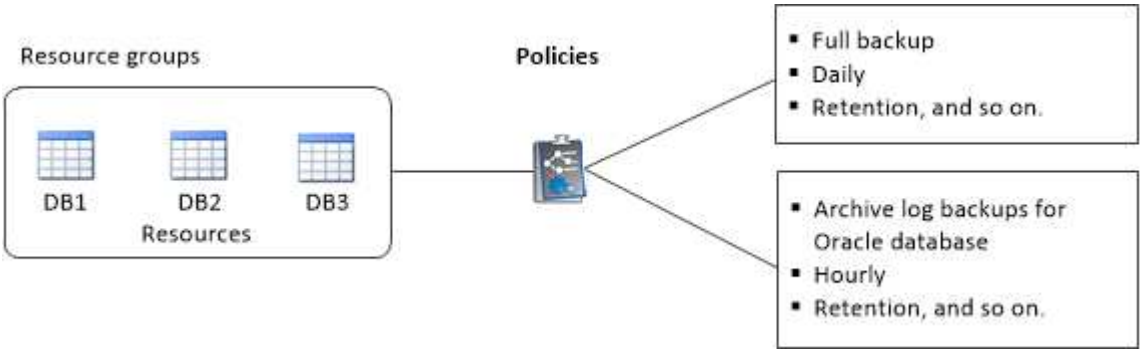
Um grupo de recursos é um contêiner onde você adiciona recursos que deseja fazer backup e proteger. Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente.

Sobre esta tarefa

- Um banco de dados com arquivos em grupos de discos ASM deve estar no estado "MONT" ou "OPEN" para verificar seus backups usando o utilitário Oracle DBVERIFY.

  Anexe uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que você deseja executar.

  A imagem a seguir ilustra o relacionamento entre recursos, grupos de recursos e políticas para bancos de dados:



- Para políticas habilitadas para SnapLock , para ONTAP 9.12.1 e versões anteriores, se você especificar um período de bloqueio de Snapshot, os clones criados a partir de Snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock . O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .
- Não há suporte para adicionar novos bancos de dados sem sincronização ativa do SnapMirror a um grupo de recursos existente que contém recursos com sincronização ativa do SnapMirror .
- Não há suporte para adicionar novos bancos de dados a um grupo de recursos existente no modo de failover da sincronização ativa do SnapMirror . Você pode adicionar recursos ao grupo de recursos

somente no estado regular ou de failback.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:
   a. Insira um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 caracteres.

   b. Insira um ou mais rótulos no campo Tag para ajudar você a pesquisar o grupo de recursos posteriormente.

      Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.

   c. Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

      Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

   d. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

      Você deve usar exatamente o mesmo destino definido no Oracle, incluindo o prefixo, se necessário.

4. Na página Recursos, selecione um nome de host do banco de dados Oracle na lista suspensa **Host**.

   Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos da seção Recursos Disponíveis e mova-os para a seção Recursos Selecionados.

   Você pode adicionar bancos de dados de hosts Linux e AIX em um único grupo de recursos.

6. Na página Configurações do aplicativo, selecione a opção de backup.
7. Na página Políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em + .

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um

agendamento.

c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

Onde *policy_name* é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Na página Verificação, execute as seguintes etapas:
   a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para realizar a verificação no armazenamento secundário.
   b. Clique na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política.
   c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name, execute as seguintes ações:

Se você quiser…	Faça isso…
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

   d. Selecione **Verificar no local secundário** para verificar seus backups no sistema de armazenamento secundário.
   e. Clique em **OK**.

Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

10. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e habilite proteção secundária para recursos Oracle em sistemas ASA r2

Você deve criar o grupo de recursos para adicionar os recursos que estão nos sistemas ASA r2. Você também pode provisionar a proteção secundária ao criar o grupo de

recursos.

Antes de começar

- Você deve garantir que não está adicionando recursos do ONTAP 9.x e recursos do ASA r2 ao mesmo grupo de recursos.
- Você deve garantir que não tenha um banco de dados com recursos ONTAP 9.x e recursos ASA r2.

Sobre esta tarefa

- A proteção secundária estará disponível somente se o usuário conectado estiver atribuído à função que tem o recurso **SecondaryProtection** habilitado.
- Se você habilitar a proteção secundária, o grupo de recursos será colocado no modo de manutenção durante a criação dos grupos de consistência primário e secundário. Depois que os grupos de consistência primário e secundário são criados, o grupo de recursos é retirado do modo de manutenção.
- O SnapCenter não oferece suporte à proteção secundária para um recurso clone.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:
   a. Insira um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 caracteres.

   b. Insira um ou mais rótulos no campo Tag para ajudar você a pesquisar o grupo de recursos posteriormente.

      Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.

   c. Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

      Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

   d. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

      Você deve usar exatamente o mesmo destino definido no aplicativo, incluindo o prefixo, se necessário.

4. Na página Recursos, selecione o nome do host do banco de dados na lista suspensa **Host**.

   Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos do ASA r2 na seção Recursos disponíveis e mova-os para a seção Recursos selecionados.
6. Na página Configurações do aplicativo, selecione a opção de backup.

7. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em + .

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

   c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

      Onde *policy_name* é o nome da política que você selecionou.

      Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

   Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Se a proteção secundária estiver habilitada para a política selecionada, a página Proteção Secundária será exibida e você precisará executar as seguintes etapas:

   a. Selecione o tipo de política de replicação.

      A política de replicação síncrona não é suportada.

   b. Especifique o sufixo do grupo de consistência que você deseja usar.

   c. Nos menus suspensos Cluster de destino e SVM de destino, selecione o cluster emparelhado e o SVM que você deseja usar.

      O cluster e o peering de SVM não são suportados pelo SnapCenter. Você deve usar o System Manager ou as CLIs do ONTAP para executar o peering de cluster e SVM.

Se os recursos já estiverem protegidos fora do SnapCenter, eles serão exibidos na seção Recursos Protegidos Secundários.

1. Na página Verificação, execute as seguintes etapas:

   a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para realizar a verificação no armazenamento secundário.

   b. Clique + na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política.

   c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name, execute as seguintes ações:

Se você quiser…	Faça isso…
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

d. Selecione **Verificar no local secundário** para verificar seus backups no sistema de armazenamento secundário.

e. Clique em **OK**.

Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

2. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

3. Revise o resumo e clique em **Concluir**.

Fazer backup de recursos Oracle

Se um recurso não fizer parte de nenhum grupo de recursos, você poderá fazer backup do recurso na página Recursos.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** na lista Exibir.
3. Clique e selecione o nome do host e o tipo de banco de dados para filtrar os recursos.

Você pode então clicar para fechar o painel de filtro.

4. Selecione o banco de dados que você deseja fazer backup.

A página Database-Protect é exibida.

5. Na página Recursos, execute as seguintes etapas:

a. Marque a caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

Por exemplo, `customtext_policy_hostname` ou `resource_hostname` . Um registro de data e hora é anexado ao nome do Snapshot por padrão.

b. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

6. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você pode criar uma política clicando em + .

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique + na coluna Configurar agendamentos para configurar um agendamento para a política desejada.

   c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione `OK` .

      policy_name é o nome da política que você selecionou.

   Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

7. Na página Verificação, execute as seguintes etapas:

   a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para verificar o armazenamento secundário.

   b. Clique + na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política. + Na caixa de diálogo Adicionar agendamentos de verificação *policy_name*, você pode executar as seguintes etapas:

   c. Selecione **Executar verificação após backup**.

   d. Selecione **Executar verificação agendada** e selecione o tipo de agendamento na lista suspensa.

      Em uma configuração do Flex ASM, não é possível executar a operação de verificação em nós Leaf se a cardinalidade for menor que o número de nós no cluster RAC.

   e. Selecione **Verificar no local secundário** para verificar seus backups no armazenamento secundário.

   f. Clique em **OK**.

      Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

8. Na página Notificação, selecione os cenários nos quais você deseja enviar os e-mails na lista suspensa **Preferência de e-mail**.

   Você deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação de backup realizada no recurso, selecione **Anexar relatório de tarefa**.

   Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando PowerShell `Set-SmSmtpServer` .

9. Revise o resumo e clique em **Concluir**.

   A página de topologia do banco de dados é exibida.

10. Clique em **Fazer backup agora**.
11. Na página Backup, execute as seguintes etapas:
    a. Se você aplicou várias políticas ao recurso, na lista suspensa Política, selecione a política que deseja usar para backup.

       Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

    b. Clique em **Backup**.
12. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Depois que você terminar

- Na configuração do AIX, você pode usar o `lkdev` comando para bloquear e o `rendev` comando para renomear os discos nos quais o banco de dados que foi feito backup estava residindo.

  Bloquear ou renomear dispositivos não afetará a operação de restauração quando você restaurar usando esse backup.

- Se a operação de backup falhar porque o tempo de execução da consulta ao banco de dados excedeu o valor de tempo limite, você deve alterar o valor dos parâmetros ORACLE_SQL_QUERY_TIMEOUT e ORACLE_PLUGIN_SQL_QUERY_TIMEOUT executando o comando `Set-SmConfigSettings` cmdlet:

  Após modificar o valor dos parâmetros, reinicie o serviço SnapCenter Plug-in Loader (SPL) executando o seguinte comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Se o arquivo não estiver acessível e o ponto de montagem não estiver disponível durante o processo de verificação, a operação poderá falhar com o código de erro DBV-00100 no arquivo especificado. Você deve modificar os valores dos parâmetros VERIFICATION_DELAY e VERIFICATION_RETRY_COUNT em sco.properties.

  Após modificar o valor dos parâmetros, reinicie o serviço SnapCenter Plug-in Loader (SPL) executando o seguinte comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Nas configurações do MetroCluster , o SnapCenter pode não conseguir detectar um relacionamento de proteção após um failover.
- Se você estiver fazendo backup de dados do aplicativo em VMDKs e o tamanho do heap Java para o SnapCenter Plug-in for VMware vSphere não for grande o suficiente, o backup poderá falhar.

  Para aumentar o tamanho do heap Java, localize o arquivo de script */opt/netapp/init_scripts/scvservice*. Nesse roteiro, o `do_start method` O comando inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: `Java -jar -Xmx8192M -Xms4096M`.

Encontre mais informações

- "Não é possível detectar o relacionamento SnapMirror ou SnapVault após failover do MetroCluster"
- "O banco de dados Oracle RAC One Node é ignorado para executar operações do SnapCenter"
- "Falha ao alterar o estado de um banco de dados Oracle 12c ASM"
- "Parâmetros personalizáveis para operações de backup, restauração e clonagem em sistemas AIX"(Requer login)

Fazer backup de grupos de recursos do banco de dados Oracle

Um grupo de recursos é uma coleção de recursos em um host ou cluster. A operação de backup é executada em todos os recursos definidos no grupo de recursos.

Você pode fazer backup de um grupo de recursos sob demanda na página Recursos. Se um grupo de recursos tiver uma política anexada e um agendamento configurado, os backups serão criados de acordo com o agendamento.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.
3. Digite o nome do grupo de recursos na caixa de pesquisa ou clique em e selecione a tag.

   Clique para fechar o painel de filtro.

4. Na página Grupo de recursos, selecione o grupo de recursos para fazer backup.

   Se você tiver um grupo de recursos federados com dois bancos de dados e um tiver dados em armazenamento não NetApp , a operação de backup será abortada mesmo que o outro banco de dados esteja no armazenamento NetApp .

5. Na página Backup, execute as seguintes etapas:
   a. Se você tiver várias políticas associadas ao grupo de recursos, selecione a política de backup que deseja usar na lista suspensa **Política**.

      Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

   b. Selecione **Backup**.
6. Monitore o progresso selecionando **Monitorar > Trabalhos**.

Depois que você terminar

- Na configuração do AIX, você pode usar o `lkdev` comando para bloquear e o `rendev` comando para renomear os discos nos quais o banco de dados que foi feito backup estava residindo.

  Bloquear ou renomear dispositivos não afetará a operação de restauração quando você restaurar usando esse backup.

- Se a operação de backup falhar porque o tempo de execução da consulta ao banco de dados excedeu o valor de tempo limite, você deve alterar o valor dos parâmetros ORACLE_SQL_QUERY_TIMEOUT e ORACLE_PLUGIN_SQL_QUERY_TIMEOUT executando o comando `Set-SmConfigSettings` cmdlet:

  Após modificar o valor dos parâmetros, reinicie o serviço SnapCenter Plug-in Loader (SPL) executando o seguinte comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Se o arquivo não estiver acessível e o ponto de montagem não estiver disponível durante o processo de verificação, a operação poderá falhar com o código de erro DBV-00100 no arquivo especificado. Você deve modificar os valores dos parâmetros VERIFICATION_DELAY_ e VERIFICATION_RETRY_COUNT em sco.properties.

Após modificar o valor dos parâmetros, reinicie o serviço SnapCenter Plug-in Loader (SPL) executando o seguinte comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

Monitorar backup do banco de dados Oracle

Aprenda a monitorar o progresso das operações de backup e proteção de dados.

Monitorar operações de backup do banco de dados Oracle

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Talvez você queira verificar o progresso para determinar quando ele foi concluído ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado correspondente das operações:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **Trabalhos**.
3. Na página Trabalhos, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de backup sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Backup**.
   d. No menu suspenso **Status**, selecione o status do backup.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione uma tarefa de backup e clique em **Detalhes** para visualizar os detalhes da tarefa.

   Embora o status do trabalho de backup seja exibido , ao clicar em detalhes do trabalho, você poderá ver que algumas das tarefas filhas da operação de backup ainda estão em andamento ou marcadas com sinais de alerta.

5. Na página Detalhes do trabalho, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Monitore as operações de proteção de dados no painel Atividade

O painel Atividade exibe as cinco operações mais recentes realizadas. O painel Atividade também exibe quando a operação foi iniciada e o status da operação.

O painel Atividade exibe informações sobre operações de backup, restauração, clonagem e backup agendado.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Clique  no painel Atividade para visualizar as cinco operações mais recentes.

   Quando você clica em uma das operações, os detalhes da operação são listados na página **Detalhes do trabalho**.

Outras operações de backup

Faça backup de bancos de dados Oracle usando comandos UNIX

O fluxo de trabalho de backup inclui planejamento, identificação de recursos para backup, criação de políticas de backup, criação de grupos de recursos e anexação de políticas, criação de backups e monitoramento das operações.

O que você vai precisar

- Você deve ter adicionado as conexões do sistema de armazenamento e criado a credencial usando os comandos *Add-SmStorageConnection* e *Add-SmCredential*.
- Você deve ter estabelecido a sessão de conexão com o SnapCenter Server usando o comando *Open-SmConnection*.

  Você pode ter apenas uma sessão de login da conta SnapCenter e o token é armazenado no diretório inicial do usuário.

  A sessão de conexão é válida apenas por 24 horas. No entanto, você pode criar um token com a opção TokenNeverExpires para criar um token que nunca expira e a sessão sempre será válida.

Sobre esta tarefa

Você deve executar os seguintes comandos para estabelecer a conexão com o SnapCenter Server, descobrir as instâncias do banco de dados Oracle, adicionar políticas e grupos de recursos, fazer backup e verificar o backup.

As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando Get-Help *command_name*. Alternativamente, você também pode consultar o "Guia de referência de comandos do software SnapCenter" .

Passos

1. Iniciar uma sessão de conexão com o SnapCenter Server para um usuário especificado: *Open-SmConnection*
2. Executar operação de descoberta de recursos do host: *Get-SmResources*
3. Configurar credenciais do banco de dados Oracle e nós preferenciais para operação de backup de um banco de dados Real Application Cluster (RAC): *Configure-SmOracleDatabase*
4. Crie uma política de backup: *Add-SmPolicy*

5. Recupere as informações sobre o local de armazenamento secundário (SnapVault ou SnapMirror): *Get-SmSecondaryDetails*

   Este comando recupera os detalhes do mapeamento de armazenamento primário para secundário de um recurso especificado. Você pode usar os detalhes do mapeamento para configurar as configurações de verificação secundárias ao criar um grupo de recursos de backup.

6. Adicionar um grupo de recursos ao SnapCenter: *Add-SmResourceGroup*
7. Criar um backup: *New-SmBackup*

   Você pode pesquisar o trabalho usando a opção WaitForCompletion. Se esta opção for especificada, o comando continuará a pesquisar o servidor até a conclusão da tarefa de backup.

8. Recuperar os logs do SnapCenter: *Get-SmLogs*

Cancelar operações de backup de bancos de dados Oracle

Você pode cancelar operações de backup que estejam em execução, na fila ou que não respondam.

Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações de backup.

Sobre esta tarefa

Quando você cancela uma operação de backup, o SnapCenter Server interrompe a operação e remove todos os Snapshots do armazenamento se o backup criado não estiver registrado no SnapCenter Server. Se o backup já estiver registrado no SnapCenter Server, ele não reverterá o Snapshot já criado, mesmo após o cancelamento ser acionado.

- Você pode cancelar somente o log ou a operação de backup completo que estão na fila ou em execução.
- Você não pode cancelar a operação após a verificação ter iniciado.

  Se você cancelar a operação antes da verificação, a operação será cancelada e a operação de verificação não será executada.

- Não é possível cancelar a operação de backup após o início das operações de catálogo.
- Você pode cancelar uma operação de backup na página Monitor ou no painel Atividade.
- Além de usar a GUI do SnapCenter , você pode usar comandos CLI para cancelar operações.
- O botão **Cancelar trabalho** fica desabilitado para operações que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de backup enfileiradas de outros membros enquanto estiver usando essa função.

Etapa

Execute uma das seguintes ações:

Do…	Ação
Página do monitor	1. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. 2. Selecione a operação e clique em **Cancelar trabalho**.
Painel de atividades	1. Após iniciar o trabalho de backup, clique em no painel Atividade para visualizar as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

Resultados

A operação é cancelada e o recurso é revertido ao estado original.

Se a operação cancelada não responder no estado de cancelamento ou execução, você deverá executar Cancel-SmJob -JobID <int> -Force para interromper à força a operação de backup.

Visualize backups e clones do banco de dados Oracle na página Topologia

Ao se preparar para fazer backup ou clonar um recurso, pode ser útil visualizar uma representação gráfica de todos os backups e clones no armazenamento primário e secundário.

Sobre esta tarefa

Na página Topologia, você pode ver todos os backups e clones disponíveis para o recurso ou grupo de recursos selecionado. Você pode visualizar os detalhes desses backups e clones e selecioná-los para executar operações de proteção de dados.

Você pode revisar os seguintes ícones na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no armazenamento primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups e clones que estão disponíveis no armazenamento primário.
- exibe o número de backups e clones que são espelhados no armazenamento secundário usando a tecnologia SnapMirror .
- exibe o número de backups e clones que são replicados no armazenamento secundário usando a tecnologia SnapVault .

  O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou 6 backups usando uma política para manter apenas 4 backups, o número de backups

exibidos será 6.

Clones de um backup de um espelho flexível em termos de versão em um volume do tipo mirror-vault são exibidos na exibição de topologia, mas a contagem de backups de espelho na exibição de topologia não inclui o backup flexível em termos de versão.

Se você tiver um relacionamento secundário como sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC]), poderá ver os seguintes ícones adicionais:

-  O site de réplica está no ar.
-  O site de réplicas está fora do ar.
-  O espelho secundário ou o relacionamento do cofre não foram restabelecidos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso na exibição de detalhes do recurso ou na exibição de detalhes do grupo de recursos.

   Se o recurso estiver protegido, a página Topologia do recurso selecionado será exibida.

4. Revise o cartão Resumo para ver um resumo do número de backups e clones disponíveis no armazenamento primário e secundário.

   A seção Cartão de Resumo exibe o número total de backups e clones e o número total de backups de log.

   Clicar no botão **Atualizar** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clicar no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Uma programação semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo estiver distribuído em vários volumes, o tempo de expiração do SnapLock para o backup será o maior tempo de expiração do SnapLock definido para um Snapshot em um volume. O maior tempo de expiração do SnapLock é recuperado do ONTAP.

   Para sincronização ativa do SnapMirror , clicar no botão **Atualizar** atualiza o inventário de backup do SnapCenter consultando o ONTAP para sites primários e de réplica. Uma programação semanal também executa essa atividade para todos os bancos de dados que contêm o relacionamento de sincronização ativo do SnapMirror .

   - Para sincronização ativa do SnapMirror e somente para o ONTAP 9.14.1, os relacionamentos Async Mirror ou Async MirrorVault com o novo destino primário devem ser configurados manualmente após o failover. A partir do ONTAP 9.15.1, o Async Mirror ou o Async MirrorVault são configurados automaticamente para o novo destino principal.
   - Após o failover, um backup deve ser criado para que o SnapCenter esteja ciente do failover. Você pode clicar em **Atualizar** somente após um backup ter sido criado.
5. Na exibição Gerenciar cópias, clique em **Backups** ou **Clones** do armazenamento primário ou secundário

para ver detalhes de um backup ou clone.

Os detalhes dos backups e clones são exibidos em formato de tabela.

6. Selecione o backup na tabela e clique nos ícones de proteção de dados para executar operações de restauração, clonagem, montagem, desmontagem, renomeação, catalogação, descatalogação e exclusão.

   Não é possível renomear ou excluir backups que estejam no armazenamento secundário.

   - Se você tiver selecionado um backup de log, você só poderá executar operações de renomeação, montagem, desmontagem, catalogação, descatalogação e exclusão.
   - Se você catalogou o backup usando o Oracle Recovery Manager (RMAN), não poderá renomear esses backups catalogados.

7. Se você quiser excluir um clone, selecione o clone na tabela e clique em .

Se o valor atribuído a SnapmirrorStatusUpdateWaitTime for menor, as cópias de backup do Mirror e do Vault não serão listadas na página de topologia, mesmo que os volumes de dados e log sejam protegidos com sucesso. Você deve aumentar o valor atribuído a SnapmirrorStatusUpdateWaitTime usando o cmdlet *Set-SmConfigSettings* do PowerShell.

As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando Get-Help *command_name*.

Alternativamente, você também pode consultar o "Guia de referência de comandos do software SnapCenter" ou "Guia de referência do cmdlet do software SnapCenter" .

Montar e desmontar backups de banco de dados

Você pode montar um ou vários backups de dados e logs somente se quiser acessar os arquivos no backup. Você pode montar o backup no mesmo host onde o backup foi criado ou em um host remoto com o mesmo tipo de Oracle e configurações de host. Se você montou os backups manualmente, deverá desmontá-los manualmente após concluir a operação. Em qualquer instância, um backup de um banco de dados pode ser montado em qualquer um dos hosts. Ao executar uma operação, você pode montar apenas um único backup.

Em uma configuração do Flex ASM, você não pode executar a operação de montagem em nós Leaf se a cardinalidade for menor que o número de nós no cluster RAC.

Montar um backup de banco de dados

Você deve montar manualmente um backup de banco de dados se quiser acessar os arquivos no backup.

O que você vai precisar

- Se você tiver uma instância de banco de dados do Automatic Storage Management (ASM) em um ambiente NFS e quiser montar os backups do ASM, deverá adicionar o caminho do disco do ASM */var/opt/snapcenter/sco/backup*/*/*/*/** ao caminho existente definido no parâmetro asm_diskstring.
- Se você tiver uma instância de banco de dados ASM em um ambiente NFS e quiser montar os backups de log do ASM como parte de uma operação de recuperação, deverá adicionar o caminho do disco ASM

/var/opt/snapcenter/scu/clones//*_* ao caminho existente definido no parâmetro asm_diskstring.

- No parâmetro asm_diskstring, você deve configurar *AFD:** se estiver usando ASMFD ou configurar *ORCL:** se estiver usando ASMLIB.

> Para obter informações sobre como editar o parâmetro asm_diskstring, consulte "Como adicionar caminhos de disco ao asm_diskstring" .

- Você deve configurar as credenciais do ASM e a porta do ASM se ela for diferente daquela do host do banco de dados de origem ao montar o backup.
- Se você quiser montar em um host alternativo, verifique se o host alternativo atende aos seguintes requisitos:
  - Mesmo UID e GID do host original
  - Mesma versão do Oracle do host original
  - Mesma distribuição e versão do sistema operacional do host original
  - Para NVMe, o utilitário NVMe deve ser instalado
- Você deve garantir que o LUN não esteja mapeado para o host AIX usando o iGroup, que consiste em protocolos mistos iSCSI e FC. Para obter mais informações, consulte "A operação falha com erro Não é possível descobrir o dispositivo para LUN" .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

   A página de topologia do banco de dados é exibida.
4. Na exibição Gerenciar cópias, selecione **Backups** do sistema de armazenamento primário ou secundário (espelhado ou replicado).
5. Selecione o backup da tabela e clique em  .
6. Na página Montar backups, selecione o host no qual você deseja montar o backup na lista suspensa **Escolha o host para montar o backup**.

   O caminho de montagem */var/opt/snapcenter/sco/backup_mount/backup_name/database_name* é exibido.

   Se você estiver montando o backup de um banco de dados ASM, o caminho de montagem +diskgroupname_SID_backupid será exibido.
7. Clique em **Montar**.

Depois que você terminar

- Você pode executar o seguinte comando para recuperar as informações relacionadas ao backup montado:

  ```
  ./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
  ```

- Se você tiver montado um banco de dados ASM, poderá executar o seguinte comando para recuperar as

informações relacionadas ao backup montado:

```
./sccli Get-Smbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
```

- Para recuperar o ID de backup, execute o seguinte comando:

  ```
  ./sccli Get-Smbackup-BackupNamebackup_name
  ```

  As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando Get-Help *command_name*. Alternativamente, você também pode consultar o "Guia de referência de comandos do software SnapCenter" .

Desmontar um backup de banco de dados

Você pode desmontar manualmente um backup de banco de dados montado quando não quiser mais acessar os arquivos no backup.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

   A página de topologia do banco de dados é exibida.

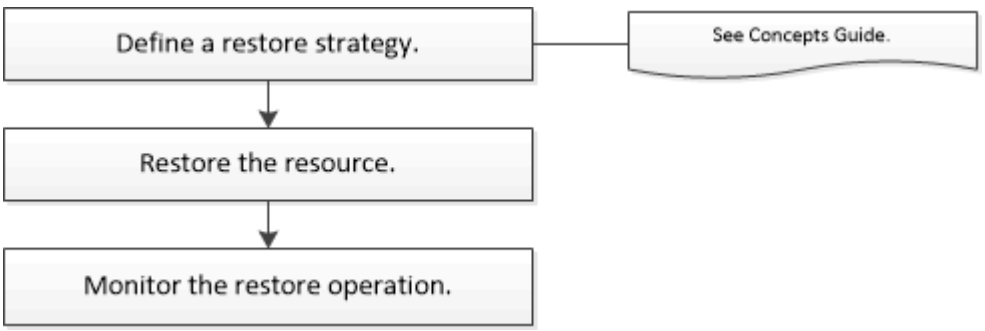
4. Selecione o backup que está montado e clique em  .
5. Clique em **OK**.

Restaurar e recuperar bancos de dados Oracle

Fluxo de trabalho de restauração

O fluxo de trabalho de restauração inclui planejamento, execução de operações de restauração e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de restauração:



Definir uma estratégia de restauração e recuperação para bancos de dados Oracle

Você deve definir uma estratégia antes de restaurar e recuperar seu banco de dados para que possa executar operações de restauração e recuperação com sucesso.

Tipos de backups suportados para operações de restauração e recuperação

O SnapCenter oferece suporte à restauração e recuperação de diferentes tipos de backups de banco de dados Oracle.

- Backup de dados online
- Backup de dados de desligamento offline
- Backup de dados de montagem offline

> Se você estiver restaurando um desligamento offline ou um backup de dados de montagem offline, o SnapCenter deixará o banco de dados em estado offline. Você deve recuperar manualmente o banco de dados e redefinir os logs.

- Backup completo
- Backups de montagem offline de bancos de dados standby do Data Guard
- Backups on-line somente de dados de bancos de dados standby do Active Data Guard

> Não é possível executar a recuperação de bancos de dados em espera do Active Data Guard.

- Backups de dados on-line, backups completos on-line, backups de montagem off-line e backups de desligamento off-line em uma configuração de Real Application Clusters (RAC)
- Backups de dados on-line, backups completos on-line, backups de montagem off-line e backups de desligamento off-line em uma configuração de Gerenciamento Automático de Armazenamento (ASM)

Tipos de métodos de restauração suportados para bancos de dados Oracle

O SnapCenter oferece suporte a conexão e cópia ou restauração no local para bancos de dados Oracle. Durante uma operação de restauração, o SnapCenter determina o método de restauração apropriado para o sistema de arquivos a ser usado para restauração sem perda de dados.

> O SnapCenter não oferece suporte ao SnapRestore baseado em volume.

Restauração de conexão e cópia

Se o layout do banco de dados for diferente do backup ou se houver novos arquivos após a criação do backup, a restauração do tipo conectar e copiar será executada. No método de restauração de conexão e cópia, as seguintes tarefas são executadas:

Passos

1. O volume é clonado do Snapshot e a pilha do sistema de arquivos é criada no host usando os LUNs ou volumes clonados.
2. Os arquivos são copiados dos sistemas de arquivos clonados para os sistemas de arquivos originais.

3. Os sistemas de arquivos clonados são então desmontados do host e os volumes clonados são excluídos do ONTAP.

> Para uma configuração Flex ASM (onde a cardinalidade é menor que o número de nós no cluster RAC) ou bancos de dados ASM RAC no VMDK ou RDM, somente o método de restauração conectar e copiar é suportado.

Mesmo que você tenha habilitado a restauração no local à força, o SnapCenter executa a restauração de conexão e cópia nos seguintes cenários:

- Restaurar do sistema de armazenamento secundário
- Restauração de grupos de discos ASM presentes em nós de uma configuração do Oracle RAC na qual a instância do banco de dados não está configurada
- Na configuração do Oracle RAC, em qualquer um dos nós pares, se a instância do ASM ou a instância do cluster não estiver em execução ou se o nó par estiver inativo
- Restauração apenas de arquivos de controle
- Restaurar um subconjunto de tablespaces que residem em um grupo de discos ASM
- O grupo de discos é compartilhado entre arquivos de dados, arquivo sp e arquivo de senha
- O serviço SnapCenter Plug-in Loader (SPL) não está instalado ou não está em execução no nó remoto em um ambiente RAC
- Novos nós são adicionados ao Oracle RAC e o SnapCenter Server não está ciente dos nós recém-adicionados

Restauração no local

Se o layout do banco de dados for semelhante ao backup e não tiver sofrido nenhuma alteração de configuração no armazenamento e na pilha do banco de dados, a restauração no local será executada, na qual a restauração do arquivo ou LUN será executada no ONTAP. O SnapCenter suporta apenas Single File SnapRestore (SFSR) como parte do método de restauração local.

> O NetApp ONTAP oferece suporte à restauração no local a partir de um local secundário.

Se você quiser executar uma restauração no local no banco de dados, certifique-se de ter apenas arquivos de dados no grupo de discos ASM. Você deve criar um backup após quaisquer alterações feitas no grupo de discos ASM ou na estrutura física do banco de dados. Após executar a restauração no local, o grupo de discos conterá o mesmo número de arquivos de dados que no momento do backup.

A restauração no local será aplicada automaticamente quando o grupo de discos ou ponto de montagem corresponder aos seguintes critérios:

- Nenhum novo arquivo de dados é adicionado após o backup (verificação de arquivo estrangeiro)
- Nenhuma adição, exclusão ou recriação de disco ASM ou LUN após o backup (verificação de alteração estrutural do grupo de discos ASM)
- Nenhuma adição, exclusão ou recriação de LUNs no grupo de discos LVM (verificação de alteração estrutural do grupo de discos LVM)

> Você também pode forçar a ativação da restauração no local usando a GUI, a CLI do SnapCenter ou o cmdlet do PowerShell para substituir a verificação de arquivo externo e a verificação de alteração estrutural do grupo de discos LVM.

Executando restauração local no ASM RAC

No SnapCenter, o nó no qual você executa a restauração é denominado nó primário e todos os outros nós do RAC nos quais o grupo de discos ASM reside são chamados de nós pares. O SnapCenter altera o estado do grupo de discos ASM para desmontar em todos os nós onde o grupo de discos ASM está no estado de montagem antes de executar a operação de restauração de armazenamento. Após a conclusão da restauração do armazenamento, o SnapCenter altera o estado do grupo de discos ASM para como estava antes da operação de restauração.

Em ambientes SAN, o SnapCenter remove dispositivos de todos os nós pares e executa a operação de desmapeamento de LUN antes da operação de restauração de armazenamento. Após a operação de restauração de armazenamento, o SnapCenter executa a operação de mapeamento de LUN e constrói dispositivos em todos os nós pares. Em um ambiente SAN, se o layout do Oracle RAC ASM estiver residindo em LUNs, durante a restauração, o SnapCenter executará operações de desmapeamento, restauração e mapeamento de LUN em todos os nós do cluster RAC onde o grupo de discos ASM reside. Antes da restauração, mesmo que todos os iniciadores dos nós RAC não tenham sido usados para os LUNs, após a restauração, o SnapCenter cria um novo iGroup com todos os iniciadores de todos os nós RAC.

- Se houver alguma falha durante a atividade de pré-restauração em nós pares, o SnapCenter reverte automaticamente o estado do grupo de discos ASM como estava antes de executar a restauração em nós pares nos quais a operação de pré-restauração foi bem-sucedida. A reversão não é suportada para o nó primário e o nó par nos quais a operação falhou. Antes de tentar outra restauração, você deve corrigir manualmente o problema no nó par e trazer o grupo de discos ASM no nó primário de volta ao estado de montagem.
- Se houver alguma falha durante a atividade de restauração, a operação de restauração falhará e nenhuma reversão será executada. Antes de tentar outra restauração, você deve corrigir manualmente o problema de restauração de armazenamento e trazer o grupo de discos ASM no nó primário de volta ao estado de montagem.
- Se houver alguma falha durante a atividade de pós-restauração em qualquer um dos nós pares, o SnapCenter continuará com a operação de restauração nos outros nós pares. Você deve corrigir manualmente o problema de pós-restauração no nó par.

Tipos de operações de restauração suportadas para bancos de dados Oracle

O SnapCenter permite que você execute diferentes tipos de operações de restauração para bancos de dados Oracle.

Antes de restaurar o banco de dados, os backups são validados para identificar se há algum arquivo faltando em comparação com os arquivos reais do banco de dados.

Restauração completa

- Restaura apenas os arquivos de dados
- Restaura apenas os arquivos de controle
- Restaura os arquivos de dados e arquivos de controle
- Restaura arquivos de dados, arquivos de controle e arquivos de log de redo nos bancos de dados Data Guard standby e Active Data Guard standby

Restauração parcial

- Restaura apenas os tablespaces selecionados
- Restaura apenas os bancos de dados plugáveis selecionados (PDBs)

- Restaura apenas os tablespaces selecionados de um PDB

Tipos de operações de recuperação suportadas para bancos de dados Oracle

O SnapCenter permite que você execute diferentes tipos de operações de recuperação para bancos de dados Oracle.

- O banco de dados até a última transação (todos os logs)
- O banco de dados até um número de alteração do sistema específico (SCN)
- O banco de dados até uma data e hora específicas

  Você deve especificar a data e a hora da recuperação com base no fuso horário do host do banco de dados.

  O SnapCenter também oferece a opção Sem recuperação para bancos de dados Oracle.

> O plug-in para banco de dados Oracle não oferece suporte à recuperação se você tiver restaurado usando um backup que foi criado com a função de banco de dados como standby. Você deve sempre executar a recuperação manual para bancos de dados físicos em espera.

Limitações relacionadas à restauração e recuperação de bancos de dados Oracle

Antes de executar operações de restauração e recuperação, você deve estar ciente das limitações.

Se você estiver usando qualquer versão do Oracle de 11.2.0.4 a 12.1.0.1, a operação de restauração ficará travada quando você executar o comando *renamedg*. Você pode aplicar o patch 19544733 da Oracle para corrigir esse problema.

As seguintes operações de restauração e recuperação não são suportadas:

- Restauração e recuperação de tablespaces do banco de dados do contêiner raiz (CDB)
- Restauração de tablespaces temporários e tablespaces temporários associados a PDBs
- Restauração e recuperação de tablespaces de vários PDBs simultaneamente
- Restauração de backups de log
- Restauração de backups para um local diferente
- Restauração de arquivos de log de refazer em qualquer configuração diferente dos bancos de dados de espera do Data Guard ou do Active Data Guard
- Restauração do arquivo SPFILE e Password
- Quando você executa uma operação de restauração em um banco de dados que foi recriado usando o nome do banco de dados preexistente no mesmo host, foi gerenciado pelo SnapCenter e tinha backups válidos, a operação de restauração substitui os arquivos de banco de dados recém-criados, mesmo que os DBIDs sejam diferentes.

  Isso pode ser evitado executando uma das seguintes ações:

  - Descubra os recursos do SnapCenter após a recriação do banco de dados
  - Crie um backup do banco de dados recriado

Limitações relacionadas à recuperação pontual de tablespaces

- A recuperação de ponto no tempo (PITR) dos tablespaces SYSTEM, SYSAUX e UNDO não é suportada
- O PITR de tablespaces não pode ser executado junto com outros tipos de restauração
- Se um tablespace for renomeado e você quiser recuperá-lo para um ponto anterior à sua renomeação, você deverá especificar o nome anterior do tablespace
- Se as restrições para as tabelas em um tablespace estiverem contidas em outro tablespace, você deverá recuperar ambos os tablespaces
- Se uma tabela e seus índices forem armazenados em tablespaces diferentes, os índices deverão ser descartados antes de executar o PITR
- O PITR não pode ser usado para recuperar o tablespace padrão atual
- O PITR não pode ser usado para recuperar tablespaces que contenham qualquer um dos seguintes objetos:
  - Objetos com objetos subjacentes (como visualizações materializadas) ou objetos contidos (como tabelas particionadas), a menos que todos os objetos subjacentes ou contidos estejam no conjunto de recuperação

    Além disso, se as partições de uma tabela particionada estiverem armazenadas em tablespaces diferentes, você deverá descartar a tabela antes de executar o PITR ou mover todas as partições para o mesmo tablespace antes de executar o PITR.

  - Desfazer ou reverter segmentos
  - Filas avançadas compatíveis com Oracle 8 com vários destinatários
  - Objetos de propriedade do usuário SYS

    Exemplos desses tipos de objetos são PL/SQL, classes Java, programas de chamada, visualizações, sinônimos, usuários, privilégios, dimensões, diretórios e sequências.

Origens e destinos para restauração de bancos de dados Oracle

Você pode restaurar um banco de dados Oracle a partir de uma cópia de backup no armazenamento primário ou secundário. Você só pode restaurar bancos de dados no mesmo local na mesma instância de banco de dados. No entanto, na configuração do Real Application Cluster (RAC), você pode restaurar bancos de dados em outros nós.

Fontes para operações de restauração

Você pode restaurar bancos de dados de um backup no armazenamento primário ou secundário. Se você quiser restaurar a partir de um backup no armazenamento secundário em uma configuração de vários espelhos, poderá selecionar o espelho do armazenamento secundário como a origem.

Destinos para operações de restauração

Você só pode restaurar bancos de dados no mesmo local na mesma instância de banco de dados.

Em uma configuração RAC, você pode restaurar bancos de dados RAC de qualquer nó no cluster.

Variáveis de ambiente predefinidas para restaurar prescrições e postscripts específicos

O SnapCenter permite que você use as variáveis de ambiente predefinidas ao executar o prescript e o postscript durante a restauração de um banco de dados.

Variáveis de ambiente predefinidas suportadas para restaurar um banco de dados

- **SC_JOB_ID** especifica o ID do trabalho da operação.

  Exemplo: 257

- **SC_ORACLE_SID** especifica o identificador do sistema do banco de dados.

  Se a operação envolver vários bancos de dados, isso conterá nomes de bancos de dados separados por barra vertical.

  Exemplo: NFSB31

- **SC_HOST** especifica o nome do host do banco de dados.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplo: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** especifica o proprietário do sistema operacional do banco de dados.

  Exemplo: oráculo

- **SC_OS_GROUP** especifica o grupo de sistema operacional do banco de dados.

  Exemplo: oinstall

- **SC_BACKUP_NAME** especifica o nome do backup.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplos:

  - Se o banco de dados não estiver sendo executado no modo ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
  - Se o banco de dados estiver sendo executado no modo ARCHIVELOG: 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** especifica o ID do backup.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplos:

  - Se o banco de dados não estiver sendo executado no modo ARCHIVELOG: DATA@203|LOG@205
  - Se o banco de dados estiver sendo executado no modo ARCHIVELOG:

DATA@203|LOG@205,206,207

- **SC_RESOURCE_GROUP_NAME** especifica o nome do grupo de recursos.

  Exemplo: RG1

- **SC_ORACLE_HOME** especifica o caminho do diretório inicial do Oracle.

  Exemplo: /ora01/app/oracle/product/18.1.0/db_1

- **SC_RECOVERY_TYPE** especifica os arquivos que serão recuperados e também o escopo da recuperação.

  Exemplo: RESTORESCOPE:usingBackupControlfile=false|RECOVERYSCOPE:allLogs=true,noLogs=false,untiltime=false,untilscn=false.

Para obter informações sobre delimitadores, consulte"Delimitadores suportados" .

Requisitos para restaurar um banco de dados Oracle

Antes de restaurar um banco de dados Oracle, você deve garantir que os pré-requisitos sejam atendidos.

- Você deve ter definido sua estratégia de restauração e recuperação.
- O administrador do SnapCenter deve ter atribuído a você as máquinas virtuais de armazenamento (SVMs) para os volumes de origem e de destino se você estiver replicando Snapshots para um espelho ou cofre.
- Se os logs de arquivamento forem removidos como parte do backup, você deverá ter montado manualmente os backups de log de arquivamento necessários.
- Se você quiser restaurar bancos de dados Oracle que residem em um Disco de Máquina Virtual (VMDK), certifique-se de que a máquina convidada tenha o número necessário de slots livres para alocar os VMDKs clonados.
- Você deve garantir que todos os volumes de dados e volumes de log de arquivamento pertencentes ao banco de dados estejam protegidos se a proteção secundária estiver habilitada para esse banco de dados.
- Você deve garantir que o banco de dados do RAC One Node esteja no estado "nomount" para executar a restauração completa do arquivo de controle ou do banco de dados.
- Se você tiver uma instância de banco de dados ASM no ambiente NFS, adicione o caminho do disco ASM */var/opt/snapcenter/scu/clones/*/** ao caminho existente definido no parâmetro asm_diskstring para montar com sucesso os backups de log do ASM como parte da operação de recuperação.
- No parâmetro asm_diskstring, você deve configurar *AFD:** se estiver usando ASMFD ou configurar *ORCL:** se estiver usando ASMLIB.

  Para obter informações sobre como editar o parâmetro asm_diskstring, consulte "Como adicionar caminhos de disco ao asm_diskstring"

- Você deve configurar o ouvinte estático no arquivo **listener.ora** disponível em *$ORACLE_HOME/network/admin* para bancos de dados não ASM e *$GRID_HOME/network/admin* para bancos de dados ASM se você desabilitou a autenticação do sistema operacional e habilitou a autenticação do banco de dados Oracle para um banco de dados Oracle e deseja restaurar os arquivos de dados e de controle desse banco de dados.

- Você deve aumentar o valor do parâmetro SCORestoreTimeout executando o comando Set-SmConfigSettings se o tamanho do banco de dados estiver em terabytes (TB).
- Você deve garantir que todas as licenças necessárias para o vCenter estejam instaladas e atualizadas.

  Se as licenças não estiverem instaladas ou atualizadas, uma mensagem de aviso será exibida. Se você ignorar o aviso e prosseguir, a restauração do RDM falhará.

- Você deve garantir que o LUN não esteja mapeado para o host AIX usando o iGroup, que consiste em protocolos mistos iSCSI e FC. Para obter mais informações, consulte "A operação falha com erro Não é possível descobrir o dispositivo para LUN" .

Restaurar e recuperar banco de dados Oracle

Em caso de perda de dados, você pode usar o SnapCenter para restaurar dados de um ou mais backups para seu sistema de arquivos ativo e, em seguida, recuperar o banco de dados.

Antes de começar

Se você instalou o plug-in como um usuário não root, deverá atribuir manualmente as permissões de execução aos diretórios prescript e postscript.

Sobre esta tarefa

- A recuperação é realizada usando os logs de arquivamento disponíveis no local de log de arquivamento configurado. Se o banco de dados estiver sendo executado no modo ARCHIVELOG, o banco de dados Oracle salvará os grupos preenchidos de arquivos de log de redo em um ou mais destinos offline, conhecidos coletivamente como log de redo arquivado. O SnapCenter identifica e monta o número ideal de backups de log com base no SCN especificado, na data e hora selecionadas ou na opção de todos os logs. Se os logs de arquivamento necessários para recuperação não estiverem disponíveis no local configurado, você deverá montar o Snapshot contendo os logs e especificar o caminho como logs de arquivamento externos.

  Se você migrar o banco de dados ASM do ASMLIB para o ASMFD, os backups criados com o ASMLIB não poderão ser usados para restaurar o banco de dados. Você deve criar backups na configuração do ASMFD e usá-los para restaurar. Da mesma forma, se o banco de dados ASM for migrado do ASMFD para o ASMLIB, você deverá criar backups na configuração do ASMLIB para restaurar.

  Ao restaurar um banco de dados, um arquivo de bloqueio operacional (.sm_lock_dbsid) é criado no host do banco de dados Oracle no diretório */var/opt/snapcenter/sco/lock* para evitar que várias operações sejam executadas no banco de dados. Após a restauração do banco de dados, o arquivo de bloqueio operacional é removido automaticamente.

  A restauração de arquivos SPFILE e Password não é suportada.

- Para políticas habilitadas para SnapLock , para ONTAP 9.12.1 e versões anteriores, se você especificar um período de bloqueio de Snapshot, os clones criados a partir de Snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock . O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.

2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

   A página de topologia do banco de dados é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
5. Selecione o backup da tabela e clique em *  *.
6. Na página Escopo de restauração, execute as seguintes tarefas:

   a. Se você selecionou um backup de um banco de dados em um ambiente Real Application Clusters (RAC), selecione o nó RAC.

   b. Quando você seleciona dados espelhados ou de cofre:

      - se não houver backup de log no espelho ou no cofre, nada será selecionado e os localizadores estarão vazios.
      - se houver backups de log no espelho ou no cofre, o backup de log mais recente será selecionado e o localizador correspondente será exibido.

      Se o backup de log selecionado existir no espelho e no cofre, ambos os localizadores serão exibidos.

   c. Execute as seguintes ações:

Se você deseja restaurar…	**Faça isso…**
Todos os arquivos de dados do banco de dados	Selecione **Todos os arquivos de dados**. Somente os arquivos de dados do banco de dados são restaurados. Os arquivos de controle, logs de arquivamento ou arquivos de log de refazer não são restaurados.
Espaços de tabela	Selecione **Tablespaces**. Você pode especificar os tablespaces que deseja restaurar.

Se você deseja restaurar…	Faça isso…
Arquivos de controle	Selecione **Arquivos de controle**. Ao restaurar os arquivos de controle, certifique-se de que a estrutura de diretório exista ou deva ser criada com as propriedades corretas de usuário e grupo, se houver, para permitir que os arquivos sejam copiados para o local de destino pelo processo de restauração. Se o diretório não existir, a tarefa de restauração falhará.
Arquivos de log de refazer	Selecione **Refazer arquivos de log**. Esta opção está disponível somente para bancos de dados Data Guard standby ou Active Data Guard standby. Os arquivos de log de refazer não são copiados para bancos de dados que não sejam do Data Guard. Para bancos de dados que não sejam do Data Guard, a recuperação é realizada usando logs de arquivamento.
Bancos de dados plugáveis (PDBs)	Selecione **Bancos de dados conectáveis** e especifique os PDBs que você deseja restaurar.
Espaços de tabela de banco de dados conectáveis (PDB)	Selecione **Tablespaces de banco de dados conectáveis (PDB)** e especifique o PDB e os tablespaces desse PDB que você deseja restaurar. Esta opção só estará disponível se você tiver selecionado um PDB para restauração.

d. Selecione **Alterar estado do banco de dados, se necessário, para restauração e recuperação** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.

   Os vários estados de um banco de dados, do mais alto ao mais baixo, são aberto, montado, iniciado e desligado. Você deve selecionar esta caixa de seleção se o banco de dados estiver em um estado superior, mas o estado deve ser alterado para um estado inferior para executar uma operação de restauração. Se o banco de dados estiver em um estado inferior, mas o estado precisar ser alterado para um estado superior para executar a operação de restauração, o estado do banco de dados será alterado automaticamente, mesmo que você não marque a caixa de seleção.

Se um banco de dados estiver no estado aberto e, para restauração, o banco de dados precisar estar no estado montado, o estado do banco de dados será alterado somente se você marcar esta caixa de seleção.

a. Selecione **Forçar restauração no local** se desejar executar a restauração no local em cenários onde novos arquivos de dados são adicionados após o backup ou quando LUNs são adicionados, excluídos ou recriados em um grupo de discos LVM.

7. Na página Escopo de Recuperação, execute as seguintes ações:

Se você…	Faça isso…
Deseja recuperar a última transação	Selecione **Todos os registros**.
Deseja recuperar para um Número de Alteração do Sistema (SCN) específico	Selecione **Até SCN (Número de alteração do sistema)**.
Deseja recuperar para uma data e hora específicas	Selecione **Data e Hora**. Você deve especificar a data e a hora do fuso horário do host do banco de dados.
Não quero recuperar	Selecione **Sem recuperação**.
Deseja especificar quaisquer locais de log de arquivo externo	Se o banco de dados estiver sendo executado no modo ARCHIVELOG, o SnapCenter identificará e montará o número ideal de backups de log com base no SCN especificado, na data e hora selecionadas ou na opção de todos os logs. Se você ainda quiser especificar o local dos arquivos de log de arquivamento externo, selecione **Especificar locais de log de arquivamento externo**. Se os logs de arquivamento forem removidos como parte do backup e você tiver montado manualmente os backups de log de arquivamento necessários, será necessário especificar o caminho do backup montado como o local do log de arquivamento externo para recuperação. Você deve verificar o caminho e o conteúdo do caminho de montagem antes de listá-lo como um local de log externo. • "Proteção de dados Oracle com ONTAP" • "A operação falha com o erro ORA-00308"

Não é possível executar a restauração com recuperação de backups secundários se os volumes de log de arquivamento não estiverem protegidos, mas os volumes de dados estiverem protegidos. Você pode

restaurar somente selecionando **Sem recuperação**.

Se você estiver recuperando um banco de dados RAC com a opção de banco de dados aberto selecionada, somente a instância do RAC onde a operação de recuperação foi iniciada será trazida de volta ao estado aberto.

> A recuperação não é suportada para bancos de dados Data Guard standby e Active Data Guard standby.

8. Na página PreOps, insira o caminho e os argumentos da prescrição que você deseja executar antes da operação de restauração.

   Você deve armazenar as prescrições no caminho */var/opt/snapcenter/spl/scripts* ou em qualquer pasta dentro desse caminho. Por padrão, o caminho */var/opt/snapcenter/spl/scripts* é preenchido. Se você criou alguma pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

   Você também pode especificar o valor do tempo limite do script. O valor padrão é 60 segundos.

   O SnapCenter permite que você use as variáveis de ambiente predefinidas ao executar o prescript e o postscript."Saber mais"

9. Na página PostOps, execute as seguintes etapas:

   a. Insira o caminho e os argumentos do postscript que você deseja executar após a operação de restauração.

      Você deve armazenar os postscripts em */var/opt/snapcenter/spl/scripts* ou em qualquer pasta dentro deste caminho. Por padrão, o caminho */var/opt/snapcenter/spl/scripts* é preenchido. Se você criou alguma pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

      > Se a operação de restauração falhar, os postscripts não serão executados e as atividades de limpeza serão acionadas diretamente.

   b. Marque a caixa de seleção se desejar abrir o banco de dados após a recuperação.

      Após restaurar um banco de dados de contêiner (CDB) com ou sem arquivos de controle, ou após restaurar apenas os arquivos de controle do CDB, se você especificar a abertura do banco de dados após a recuperação, somente o CDB será aberto e não os bancos de dados conectáveis (PDB) nesse CDB.

      Em uma configuração RAC, somente a instância RAC usada para recuperação é aberta após a recuperação.

      > Após restaurar um tablespace de usuário com arquivos de controle, um tablespace de sistema com ou sem arquivos de controle ou um PDB com ou sem arquivos de controle, somente o estado do PDB relacionado à operação de restauração é alterado para o estado original. O estado dos outros PDBs que não foram usados para restauração não são alterados para o estado original porque o estado desses PDBs não foi salvo. Você deve alterar manualmente o estado dos PDBs que não foram usados para restauração.

10. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar as notificações por e-mail.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação de restauração realizada, selecione **Anexar relatório de tarefa**.

Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

11. Revise o resumo e clique em **Concluir**.
12. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Para mais informações

- "O banco de dados Oracle RAC One Node é ignorado para executar operações do SnapCenter"
- "Falha ao restaurar de um local secundário do SnapMirror ou SnapVault"
- "Falha ao restaurar a partir de um backup de uma encarnação órfã"
- "Parâmetros personalizáveis para operações de backup, restauração e clonagem em sistemas AIX"

Restaurar e recuperar tablespaces usando recuperação de ponto no tempo

Você pode restaurar um subconjunto de tablespaces que foi corrompido ou descartado sem afetar os outros tablespaces no banco de dados. O SnapCenter usa o RMAN para executar a recuperação de ponto no tempo (PITR) dos tablespaces.

Antes de começar

- Os backups necessários para executar o PITR de tablespaces devem ser catalogados e montados.
- Se você instalou o plug-in como um usuário não root, deverá atribuir manualmente as permissões de execução aos diretórios prescript e postscript.

Sobre esta tarefa

Durante a operação PITR, o RMAN cria uma instância auxiliar no destino auxiliar especificado. O destino auxiliar pode ser um ponto de montagem ou um grupo de discos ASM. Se houver espaço suficiente no local montado, você poderá reutilizar um dos locais montados em vez de um ponto de montagem dedicado.

Você deve especificar a data e a hora ou SCN e o tablespace será restaurado no banco de dados de origem.

Você pode selecionar e restaurar vários tablespaces residentes em ambientes ASM, NFS e SAN. Por exemplo, se os tablespaces TS2 e TS3 residirem no NFS e o TS4 residir no SAN, você poderá executar uma única operação PITR para restaurar todos os tablespaces.

Em uma configuração RAC, você pode executar PITR de tablespaces de qualquer nó do RAC.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados do tipo instância única (multilocatário) na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

A página de topologia do banco de dados é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).

   Se o backup não estiver catalogado, você deve selecioná-lo e clicar em **Catálogo**.

5. Selecione o backup catalogado e clique em *  *.
6. Na página Escopo de restauração, execute as seguintes tarefas:
   a. Se você selecionou um backup de um banco de dados em um ambiente Real Application Clusters (RAC), selecione o nó RAC.
   b. Selecione **Tablespaces** e especifique os tablespaces que deseja restaurar.

      Não é possível executar PITR nos tablespaces SYSAUX, SYSTEM e UNDO.

   c. Selecione **Alterar estado do banco de dados, se necessário, para restauração e recuperação** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.
7. Na página Escopo de Recuperação, execute uma das seguintes ações:
   - Se você quiser recuperar para um Número de Alteração do Sistema (SCN) específico, selecione **Até SCN** e especifique o SCN e o destino auxiliar.
   - Se você quiser recuperar para uma data e hora específicas, selecione **Data e Hora** e especifique a data, a hora e o destino auxiliar.

     O SnapCenter identifica, monta e cataloga o número ideal de backups de dados e logs necessários para executar o PITR com base no SCN especificado ou na data e hora selecionadas.
8. Na página PreOps, insira o caminho e os argumentos da prescrição que você deseja executar antes da operação de restauração.

   Você deve armazenar as prescrições no caminho /var/opt/snapcenter/spl/scripts ou em qualquer pasta dentro desse caminho. Por padrão, o caminho /var/opt/snapcenter/spl/scripts é preenchido. Se você criou alguma pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

   Você também pode especificar o valor do tempo limite do script. O valor padrão é 60 segundos.

   O SnapCenter permite que você use as variáveis de ambiente predefinidas ao executar o prescript e o postscript."Saber mais"
9. Na página PostOps, execute as seguintes etapas:
   a. Insira o caminho e os argumentos do postscript que você deseja executar após a operação de restauração.

      Se a operação de restauração falhar, os postscripts não serão executados e as atividades de limpeza serão acionadas diretamente.

   b. Marque a caixa de seleção se desejar abrir o banco de dados após a recuperação.
10. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar as notificações por e-mail.

11. Revise o resumo e clique em **Concluir**.
12. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Restaurar e recuperar banco de dados plugável usando recuperação de ponto no tempo

Você pode restaurar e recuperar um banco de dados conectável (PDB) que foi corrompido ou descartado sem afetar os outros PDBs no banco de dados do contêiner (CDB). O SnapCenter usa o RMAN para executar a recuperação de ponto no tempo (PITR) do PDB.

Antes de começar

- Os backups necessários para executar o PITR de um PDB devem ser catalogados e montados.

  Em uma configuração RAC, você deve fechar manualmente o PDB (alterando o estado para MONTADO) em todos os nós da configuração RAC.

- Se você instalou o plug-in como um usuário não root, deverá atribuir manualmente as permissões de execução aos diretórios prescript e postscript.

Sobre esta tarefa

Durante a operação PITR, o RMAN cria uma instância auxiliar no destino auxiliar especificado. O destino auxiliar pode ser um ponto de montagem ou um grupo de discos ASM. Se houver espaço suficiente no local montado, você poderá reutilizar um dos locais montados em vez de um ponto de montagem dedicado.

Você deve especificar a data e a hora ou SCN para executar o PITR do PDB. O RMAN pode recuperar PDBs de LEITURA E GRAVAÇÃO, SOMENTE LEITURA ou descartados, incluindo arquivos de dados.

Você pode restaurar e recuperar apenas:

- um PDB de cada vez
- um tablespace em um PDB
- vários tablespaces do mesmo PDB

Em uma configuração RAC, você pode executar PITR de tablespaces de qualquer nó do RAC.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados do tipo instância única (multilocatário) na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

   A página de topologia do banco de dados é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).

   Se o backup não estiver catalogado, você deve selecioná-lo e clicar em **Catálogo**.

5. Selecione o backup catalogado e clique em *  *.
6. Na página Escopo de restauração, execute as seguintes tarefas:
   a. Se você selecionou um backup de um banco de dados em um ambiente Real Application Clusters (RAC), selecione o nó RAC.
   b. Dependendo se você deseja restaurar o PDB ou os tablespaces em um PDB, execute uma das ações:

Se você quiser…	Passos…
Restaurar um PDB	i. Selecione **Bancos de dados conectáveis (PDBs)**. ii. Especifique o PDB que você deseja restaurar. Não é possível executar PITR no banco de dados PDB$SEED.
Restaurar tablespaces em um PDB	i. Selecione **Tablespaces de banco de dados conectáveis (PDB)**. ii. Especifique o PDB. iii. Especifique um único tablespace ou vários tablespaces que você deseja restaurar. Não é possível executar PITR nos tablespaces SYSAUX, SYSTEM e UNDO.

   c. Selecione **Alterar estado do banco de dados, se necessário, para restauração e recuperação** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.
7. Na página Escopo de Recuperação, execute uma das seguintes ações:
   - Se você quiser recuperar para um Número de Alteração do Sistema (SCN) específico, selecione **Até SCN** e especifique o SCN e o destino auxiliar.
   - Se você quiser recuperar para uma data e hora específicas, selecione **Data e Hora** e especifique a data, a hora e o destino auxiliar.

     O SnapCenter identifica, monta e cataloga o número ideal de backups de dados e logs necessários para executar o PITR com base no SCN especificado ou na data e hora selecionadas.
8. Na página PreOps, insira o caminho e os argumentos da prescrição que você deseja executar antes da operação de restauração.

   Você deve armazenar as prescrições no caminho /var/opt/snapcenter/spl/scripts ou em qualquer pasta dentro desse caminho. Por padrão, o caminho /var/opt/snapcenter/spl/scripts é preenchido. Se você criou alguma pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

Você também pode especificar o valor do tempo limite do script. O valor padrão é 60 segundos.

O SnapCenter permite que você use as variáveis de ambiente predefinidas ao executar o prescript e o postscript."Saber mais"

9. Na página PostOps, execute as seguintes etapas:
   a. Insira o caminho e os argumentos do postscript que você deseja executar após a operação de restauração.

      Se a operação de restauração falhar, os postscripts não serão executados e as atividades de limpeza serão acionadas diretamente.

   b. Marque a caixa de seleção se desejar abrir o banco de dados após a recuperação.

      Em uma configuração RAC, o PDB será aberto somente no nó onde o banco de dados foi recuperado. Você deve abrir manualmente o PDB recuperado em todos os outros nós da configuração do RAC.
10. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar as notificações por e-mail.
11. Revise o resumo e clique em **Concluir**.
12. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Restaurar e recuperar bancos de dados Oracle usando comandos UNIX

O fluxo de trabalho de restauração e recuperação inclui planejamento, execução de operações de restauração e recuperação e monitoramento das operações.

Sobre esta tarefa

- Você deve executar os seguintes comandos para estabelecer a conexão com o SnapCenter Server, listar os backups, recuperar suas informações e restaurar o backup.

  As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando Get-Help *command_name*. Alternativamente, você também pode consultar o "Guia de referência de comandos do software SnapCenter" .

- Para a operação de restauração de sincronização ativa do SnapMirror , você deve selecionar o backup do local principal.

Passos

1. Iniciar uma sessão de conexão com o SnapCenter Server para um usuário especificado: *Open-SmConnection*
2. Recupere as informações sobre os backups que você deseja restaurar: *Get-SmBackup*
3. Recupere as informações detalhadas sobre o backup especificado: *Get-SmBackupDetails*

   Este comando recupera informações detalhadas sobre o backup de um recurso especificado com um ID de backup fornecido. As informações incluem nome do banco de dados, versão, SCN inicial e final, tablespaces, bancos de dados plugáveis e seus tablespaces.

4. Restaurar dados do backup: *Restore-SmBackup*

Monitorar operações de restauração do banco de dados Oracle

Você pode monitorar o progresso de diferentes operações de restauração do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa tomar.

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de restauração sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Restaurar**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Aplicar** para visualizar as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Cancelar operações de restauração do banco de dados Oracle

Você pode cancelar trabalhos de restauração que estão na fila.

Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações de restauração.

Sobre esta tarefa

- Você pode cancelar uma operação de restauração enfileirada na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de restauração em execução.

- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de restauração enfileiradas.
- O botão **Cancelar tarefa** fica desabilitado para operações de restauração que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de restauração enfileiradas de outros membros enquanto estiver usando essa função.

Etapa

Execute uma das seguintes ações:

Do…	Ação
Página do monitor	1. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. 2. Selecione o trabalho e clique em **Cancelar trabalho**.
Painel de atividades	1. Após iniciar a operação de restauração, clique em no painel Atividade para visualizar as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

Clonar banco de dados Oracle

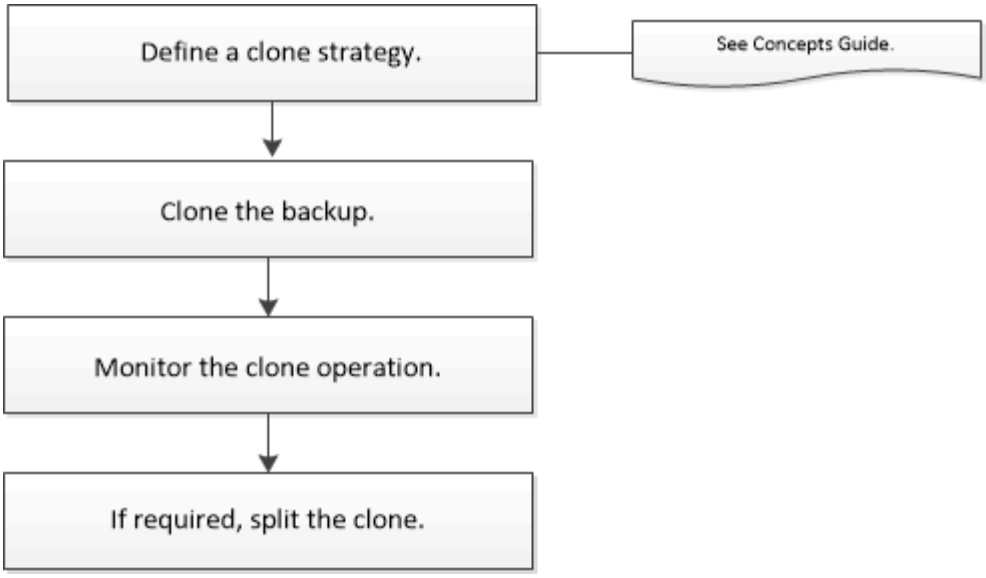
Fluxo de trabalho de clonagem

O fluxo de trabalho do clone inclui o planejamento, a execução da operação de clone e o monitoramento da operação.

Você pode clonar bancos de dados pelos seguintes motivos:

- Para testar a funcionalidade que precisa ser implementada usando a estrutura e o conteúdo atuais do banco de dados durante os ciclos de desenvolvimento do aplicativo.
- Para preencher data warehouses usando ferramentas de extração e manipulação de dados.
- Para recuperar dados que foram excluídos ou alterados por engano.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de clonagem:



Definir uma estratégia de clone para bancos de dados Oracle

Definir uma estratégia antes de clonar seu banco de dados garante que a operação de clonagem seja bem-sucedida.

Tipos de backups suportados para clonagem

O SnapCenter suporta a clonagem de diferentes tipos de backups de bancos de dados Oracle.

- Backup de dados online
- Backup completo online
- Backup de montagem offline
- Backup de desligamento offline
- Backups de bancos de dados standby do Data Guard e bancos de dados standby do Active Data Guard
- Backups de dados on-line, backups completos on-line, backups de montagem off-line e backups de desligamento off-line em uma configuração de Real Application Clusters (RAC)
- Backups de dados on-line, backups completos on-line, backups de montagem off-line e backups de desligamento off-line em uma configuração de Gerenciamento Automático de Armazenamento (ASM)

As configurações SAN não serão suportadas se a opção user_friendly_names no arquivo de configuração multipath estiver definida como sim.

A clonagem de backups de log de arquivo não é suportada.

Tipos de clonagem suportados para bancos de dados Oracle

Em um ambiente de banco de dados Oracle, o SnapCenter oferece suporte à clonagem de um backup de banco de dados. Você pode clonar o backup de sistemas de armazenamento primário e secundário.

O SnapCenter Server usa a tecnologia NetApp FlexClone para clonar backups.

Você pode atualizar um clone executando o comando "Refresh-SmClone". Este comando cria um backup do

banco de dados, exclui o clone existente e cria um clone com o mesmo nome.

A operação de atualização do clone só pode ser executada usando os comandos UNIX.

Convenções de nomenclatura de clones para bancos de dados Oracle

A partir do SnapCenter 3.0, a convenção de nomenclatura usada para clones de sistemas de arquivos é diferente dos clones de grupos de discos ASM.

- A convenção de nomenclatura para sistemas de arquivos SAN ou NFS é FileSystemNameofsourcedatabase_CLONESID.
- A convenção de nomenclatura para grupos de discos ASM é SC_HASHCODEofDISKGROUP_CLONESID.

  HASHCODEofDISKGROUP é um número gerado automaticamente (2 a 10 dígitos) que é exclusivo para cada grupo de discos ASM.

Limitações da clonagem de bancos de dados Oracle

Você deve estar ciente das limitações das operações de clonagem antes de clonar os bancos de dados.

- Se você estiver usando qualquer versão do Oracle de 11.2.0.4 a 12.1.0.1, a operação de clonagem ficará travada quando você executar o comando *renamedg*. Você pode aplicar o patch 19544733 da Oracle para corrigir esse problema.
- A clonagem de bancos de dados de um LUN diretamente conectado a um host (por exemplo, usando o Microsoft iSCSI Initiator em um host Windows) para um VMDK ou um LUN RDM no mesmo host Windows ou em outro host Windows, ou vice-versa, não é suportada.
- O diretório raiz do ponto de montagem do volume não pode ser um diretório compartilhado.
- Se você mover um LUN que contém um clone para um novo volume, o clone não poderá ser excluído.

Variáveis de ambiente predefinidas para prescript e postscript específicos do clone

O SnapCenter permite que você use as variáveis de ambiente predefinidas ao executar o prescript e o postscript ao clonar um banco de dados.

Variáveis de ambiente predefinidas suportadas para clonagem de banco de dados

- **SC_ORIGINAL_SID** especifica o SID do banco de dados de origem.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplo: NFSB32

- **SC_ORIGINAL_HOST** especifica o nome do host de origem.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplo: asmrac1.gdl.englab.netapp.com

- **SC_ORACLE_HOME** especifica o caminho do diretório inicial do Oracle do banco de dados de destino.

  Exemplo: /ora01/app/oracle/product/18.1.0/db_1

- **SC_BACKUP_NAME**" especifica o nome do backup.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplos:

  - Se o banco de dados não estiver sendo executado no modo ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
  - Se o banco de dados estiver sendo executado no modo ARCHIVELOG: 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_AV_NAME** especifica os nomes dos volumes do aplicativo.

  Exemplo: AV1|AV2
- **SC_ORIGINAL_OS_USER** especifica o proprietário do sistema operacional do banco de dados de origem.

  Exemplo: oráculo
- **SC_ORIGINAL_OS_GROUP** especifica o grupo do sistema operacional do banco de dados de origem.

  Exemplo: oinstall
- **SC_TARGET_SID**" especifica o SID do banco de dados clonado.

  Para o fluxo de trabalho de clone do PDB, o valor deste parâmetro não será predefinido.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplo: clonedb
- **SC_TARGET_HOST** especifica o nome do host onde o banco de dados será clonado.

  Este parâmetro será preenchido para volumes de aplicativos.

  Exemplo: asmrac1.gdl.englab.netapp.com
- **SC_TARGET_OS_USER** especifica o proprietário do sistema operacional do banco de dados clonado.

  Para o fluxo de trabalho de clone do PDB, o valor deste parâmetro não será predefinido.

  Exemplo: oráculo
- **SC_TARGET_OS_GROUP** especifica o grupo de sistema operacional do banco de dados clonado.

  Para o fluxo de trabalho de clone do PDB, o valor deste parâmetro não será predefinido.

  Exemplo: oinstall
- **SC_TARGET_DB_PORT** especifica a porta do banco de dados clonado.

  Para o fluxo de trabalho de clone do PDB, o valor deste parâmetro não será predefinido.

Exemplo: 1521

Para obter informações sobre delimitadores, consulte"Delimitadores suportados" .

Requisitos para clonar um banco de dados Oracle

Antes de clonar um banco de dados Oracle, você deve garantir que os pré-requisitos sejam atendidos.

- Você deve ter criado um backup do banco de dados usando o SnapCenter.

  Você deve ter criado com sucesso backups de dados e logs on-line ou backups off-line (montagem ou desligamento) para que a operação de clonagem seja bem-sucedida.

- Se você quiser personalizar os caminhos do arquivo de controle ou do arquivo de log de refazer, deverá ter pré-provisionado o sistema de arquivos necessário ou o grupo de discos do Gerenciamento Automático de Armazenamento (ASM).

  Por padrão, os arquivos de log de refazer e de controle do banco de dados clonado são criados no grupo de discos ASM ou no sistema de arquivos provisionado pelo SnapCenter para os arquivos de dados do banco de dados clone.

- Se estiver usando ASM sobre NFS, você deve adicionar */var/opt/snapcenter/scu/clones/*/** ao caminho existente definido no parâmetro asm_diskstring.
- No parâmetro asm_diskstring, você deve configurar *AFD:** se estiver usando ASMFD ou configurar *ORCL:** se estiver usando ASMLIB.

  Para obter informações sobre como editar o parâmetro asm_diskstring, consulte "Como adicionar caminhos de disco ao asm_diskstring" .

- Se você estiver criando o clone em um host alternativo, o host alternativo deverá atender aos seguintes requisitos:
  - O plug-in SnapCenter para Oracle Database deve ser instalado no host alternativo.
  - O host clone deve ser capaz de descobrir LUNs do armazenamento primário ou secundário.
    - Se você estiver clonando do armazenamento primário ou secundário (Vault ou Mirror) para um host alternativo, certifique-se de que uma sessão iSCSI seja estabelecida entre o armazenamento secundário e o host alternativo ou zoneada corretamente para FC.
    - Se você estiver clonando do armazenamento Vault ou Mirror para o mesmo host, certifique-se de que uma sessão iSCSI esteja estabelecida entre o armazenamento Vault ou Mirror e o host, ou zoneada corretamente para FC.
    - Se você estiver clonando em um ambiente virtualizado, certifique-se de que uma sessão iSCSI seja estabelecida entre o armazenamento primário ou secundário e o servidor ESX que hospeda o host alternativo, ou zoneada corretamente para FC.

      Para obter informações, consulte "documentação de utilitários de host" .

  - Se o banco de dados de origem for um banco de dados ASM:
    - A instância do ASM deve estar ativa e em execução no host onde o clone será executado.
    - O grupo de discos ASM deve ser provisionado antes da operação de clonagem se você quiser colocar arquivos de log de arquivamento do banco de dados clonado em um grupo de discos ASM

dedicado.

- O nome do grupo de discos de dados pode ser configurado, mas certifique-se de que o nome não seja usado por nenhum outro grupo de discos ASM no host onde a clonagem será executada.

  Os arquivos de dados que residem no grupo de discos ASM são provisionados como parte do fluxo de trabalho de clonagem do SnapCenter .

- Para NVMe, o utilitário NVMe deve ser instalado

- O tipo de proteção para o LUN de dados e o LUN de log, como espelho, cofre ou espelho-cofre, deve ser o mesmo para descobrir localizadores secundários durante a clonagem para um host alternativo usando backups de log.
- Você deve definir o valor de exclude_seed_cdb_view como FALSE no arquivo de parâmetros do banco de dados de origem para recuperar informações relacionadas ao PDB de seed para clonar um backup do banco de dados 12_c_.

  O PDB semente é um modelo fornecido pelo sistema que o CDB pode usar para criar PDBs. O PDB semente é chamado PDB$SEED. Para obter informações sobre PDB$SEED, consulte o Oracle Doc ID 1940806.1.

  Você deve definir o valor antes de fazer backup do banco de dados 12_c_.

- O SnapCenter suporta backup de sistemas de arquivos gerenciados pelo subsistema autofs. Se você estiver clonando o banco de dados, certifique-se de que os pontos de montagem de dados não estejam na raiz do ponto de montagem do autofs, porque o usuário raiz do host do plug-in não tem permissão para criar diretórios na raiz do ponto de montagem do autofs.

  Se os arquivos de log de controle e refazer estiverem no ponto de montagem de dados, você deverá modificar o caminho do arquivo de controle e, em seguida, o caminho do arquivo de log de refazer adequadamente.

  Você pode registrar manualmente os novos pontos de montagem clonados com o subsistema autofs. Os novos pontos de montagem clonados não serão registrados automaticamente.

- Se você tiver um TDE (login automático) e quiser clonar o banco de dados no mesmo host ou em um host alternativo, você deve copiar a carteira (arquivos de chave) em */etc/ORACLE/WALLET/$ORACLE_SID* do banco de dados de origem para o banco de dados clonado.
- Você deve definir o valor de use_lvmetad = 0 em */etc/lvm/lvm.conf* e parar o serviço lvm2-lvmetad para executar com sucesso a clonagem em ambientes de rede de área de armazenamento (SAN) no Oracle Linux 7 ou posterior ou no Red Hat Enterprise Linux (RHEL) 7 ou posterior.
- Você deve instalar o patch 13366202 do Oracle se estiver usando o banco de dados Oracle 11.2.0.3 ou posterior e o ID do banco de dados para a instância auxiliar for alterado usando um script NID.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de armazenamento (SVM).
- Para NVMe, se alguma porta de destino tiver que ser excluída da conexão, você deve adicionar o nome do nó de destino e o nome da porta no arquivo /var/opt/snapcenter/scu/etc/nvme.conf.

  Se o arquivo não existir, você deve criá-lo conforme mostrado no exemplo abaixo:

```
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>
}
```

- Você deve garantir que o LUN não esteja mapeado para o host AIX usando o iGroup, que consiste em protocolos mistos iSCSI e FC. Para obter mais informações, consulte "A operação falha com erro Não é possível descobrir o dispositivo para LUN" .

Clonar um backup de banco de dados Oracle

Você pode usar o SnapCenter para clonar um banco de dados Oracle usando o backup do banco de dados.

Antes de começar

Se você instalou o plug-in como um usuário não root, deverá atribuir manualmente as permissões de execução aos diretórios prescript e postscript.

Sobre esta tarefa

- A operação de clonagem cria uma cópia dos arquivos de dados do banco de dados e cria novos arquivos de log de refazer on-line e arquivos de controle. O banco de dados pode ser recuperado opcionalmente em um horário específico, com base nas opções de recuperação especificadas.

  A clonagem falhará se você tentar clonar um backup criado em um host Linux para um host AIX ou vice-versa.

  O SnapCenter cria um banco de dados independente quando clonado de um backup de banco de dados Oracle RAC. O SnapCenter oferece suporte à criação de clones a partir do backup de um banco de dados Data Guard standby e Active Data Guard standby.

  Durante a clonagem, o SnapCenter monta o número ideal de backups de log com base no SCN ou data e hora para operações de recuperação. Após a recuperação, o backup do log é desmontado. Todos esses clones são montados em */var/opt/snapcenter/scu/clones/*. Se estiver usando ASM sobre NFS, você deve adicionar */var/opt/snapcenter/scu/clones/*/** ao caminho existente definido no parâmetro asm_diskstring.

  Ao clonar um backup de um banco de dados ASM em um ambiente SAN, as regras do udev para os dispositivos host clonados são criadas em */etc/udev/rules.d/999-scu-netapp.rules*. Essas regras do udev associadas aos dispositivos host clonados são excluídas quando você exclui o clone.

  Em uma configuração do Flex ASM, você não pode executar a operação de clonagem em nós Leaf se a cardinalidade for menor que o número de nós no cluster RAC.

- Para políticas habilitadas para SnapLock , para ONTAP 9.12.1 e versões anteriores, se você especificar um período de bloqueio de Snapshot, os clones criados a partir de Snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock . O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

   A página de topologia do banco de dados é exibida.

4. Na exibição Gerenciar cópias, selecione os backups entre Cópias locais (primárias), Cópias espelhadas (secundárias) ou Cópias de cofre (secundárias).
5. Selecione o backup de dados na tabela e clique em *  *.
6. Na página Nome, execute uma das seguintes ações:

Se você quiser…	Passos…
Clonar um banco de dados (CDB ou não CDB)	a. Especifique o SID do clone. O SID clone não está disponível por padrão, e o comprimento máximo do SID é de 8 caracteres. Você deve garantir que não exista nenhum banco de dados com o mesmo SID no host onde o clone será criado.
Clonar um banco de dados plugável (PDB)	a. Selecione **PDB Clone**. b. Especifique o PDB que você deseja clonar. c. Especifique o nome do PDB clonado. Para obter as etapas detalhadas para clonar um PDB, consulte"Clonar um banco de dados plugável" .

   Quando você seleciona dados espelhados ou de cofre:

   - se não houver backup de log no espelho ou no cofre, nada será selecionado e os localizadores estarão vazios.
   - se houver backups de log no espelho ou no cofre, o backup de log mais recente será selecionado e o localizador correspondente será exibido.

     Se o backup de log selecionado existir no espelho e no cofre, ambos os localizadores serão exibidos.

7. Na página Locais, execute as seguintes ações:

Para este campo…	Faça isso…
Host clone	Por padrão, o host do banco de dados de origem é preenchido. Se você quiser criar o clone em um host alternativo, selecione o host que tenha a mesma versão do Oracle e do sistema operacional que o host do banco de dados de origem.
Localizações de arquivos de dados	Por padrão, o local do arquivo de dados é preenchido. A convenção de nomenclatura padrão do SnapCenter para sistemas de arquivos SAN ou NFS é FileSystemNameofsourcedatabase_CLONESID. A convenção de nomenclatura padrão do SnapCenter para grupos de discos ASM é SC_HASHCODEofDISKGROUP_CLONESID. O HASHCODEofDISKGROUP é um número gerado automaticamente (2 a 10 dígitos) que é exclusivo para cada grupo de discos ASM. Se você estiver personalizando o nome do grupo de discos ASM, certifique-se de que o comprimento do nome esteja de acordo com o comprimento máximo suportado pela Oracle. Se quiser especificar um caminho diferente, você deve inserir os pontos de montagem do arquivo de dados ou os nomes dos grupos de discos ASM para o banco de dados clone. Ao personalizar o caminho do arquivo de dados, você também deve alterar os nomes dos grupos de discos ASM ou do sistema de arquivos do arquivo de controle e do arquivo de log de refazer para o mesmo nome usado para arquivos de dados ou para grupos de discos ASM ou sistema de arquivos existentes.

Para este campo…	Faça isso…
Arquivos de controle	Por padrão, o caminho do arquivo de controle é preenchido. Os arquivos de controle são colocados no mesmo grupo de discos ASM ou sistema de arquivos dos arquivos de dados. Se quiser substituir o caminho do arquivo de controle, você pode fornecer um caminho de arquivo de controle diferente. O sistema de arquivos ou o grupo de discos ASM deve existir no host. Por padrão, o número de arquivos de controle será o mesmo do banco de dados de origem. Você pode modificar o número de arquivos de controle, mas é necessário no mínimo um arquivo de controle para clonar o banco de dados. Você pode personalizar o caminho do arquivo de controle para um sistema de arquivos diferente (existente) daquele do banco de dados de origem.

Para este campo…	Faça isso…
Logs de refazer	Por padrão, o grupo de arquivos de log de refazer, o caminho e seus tamanhos são preenchidos. Os logs de refazer são colocados no mesmo grupo de discos ASM ou sistema de arquivos dos arquivos de dados do banco de dados clonado. Se você quiser substituir o caminho do arquivo de log de refazer, poderá personalizá-lo para um sistema de arquivos diferente daquele do banco de dados de origem. O novo sistema de arquivos ou o grupo de discos ASM deve existir no host. Por padrão, o número de grupos de logs de redo, arquivos de log de redo e seus tamanhos serão os mesmos do banco de dados de origem. Você pode modificar os seguintes parâmetros: • Número de grupos de logs de refazer São necessários no mínimo dois grupos de logs de refazer para clonar o banco de dados. • Refazer arquivos de log em cada grupo e seu caminho Você pode personalizar o caminho do arquivo de log de refazer para um sistema de arquivos diferente (existente) daquele do banco de dados de origem. É necessário no mínimo um arquivo de log de refazer no grupo de log de refazer para clonar o banco de dados. • Tamanhos do arquivo de log de refazer

8. Na página Credenciais, execute as seguintes ações:

Para este campo…	Faça isso…
Nome da credencial para usuário sys	Selecione a credencial a ser usada para definir a senha do usuário sys do banco de dados clone. Se SQLNET.AUTHENTICATION_SERVICES estiver definido como NONE no arquivo sqlnet.ora no host de destino, você não deverá selecionar **None** como Credencial na GUI do SnapCenter .
Nome da credencial da instância ASM	Selecione **Nenhum** se a autenticação do sistema operacional estiver habilitada para conexão com a instância do ASM no host clone. Caso contrário, selecione a credencial do Oracle ASM configurada com o usuário “sys” ou um usuário com privilégio “sysasm” aplicável ao host clone.

Os detalhes do Oracle home, nome de usuário e grupo são preenchidos automaticamente a partir do banco de dados de origem. Você pode alterar os valores com base no ambiente Oracle do host onde o clone será criado.

9. Na página PreOps, execute as seguintes etapas:

   a. Insira o caminho e os argumentos da prescrição que você deseja executar antes da operação de clonagem.

      Você deve armazenar a prescrição em */var/opt/snapcenter/spl/scripts* ou em qualquer pasta dentro deste caminho. Por padrão, o caminho */var/opt/snapcenter/spl/scripts* é preenchido. Se você colocou o script em qualquer pasta dentro deste caminho, você precisa fornecer o caminho completo até a pasta onde o script está colocado.

      O SnapCenter permite que você use as variáveis de ambiente predefinidas ao executar o prescript e o postscript."Saber mais"

   b. Na seção Configurações de parâmetros do banco de dados, modifique os valores dos parâmetros do banco de dados pré-preenchidos que são usados para inicializar o banco de dados.

      Você pode adicionar parâmetros adicionais clicando em * + *.

      Se você estiver usando o Oracle Standard Edition e o banco de dados estiver sendo executado no modo de log de arquivamento ou se desejar restaurar um banco de dados a partir do log de refazer do arquivo, adicione os parâmetros e especifique o caminho.

      - DESTINO_DE_ARQUIVO_DE_LOG
      - LOG_ARQUIVO_DUPLEX_DESTINO

      > A área de recuperação rápida (FRA) não está definida nos parâmetros do banco de dados pré-preenchidos. Você pode configurar o FRA adicionando os parâmetros relacionados.

O valor padrão de log_archive_dest_1 é $ORACLE_HOME/clone_sid e os logs de arquivamento do banco de dados clonado serão criados neste local. Se você excluiu o parâmetro log_archive_dest_1, o local do log de arquivamento será determinado pelo Oracle. Você pode definir um novo local para o log de arquivamento editando log_archive_dest_1, mas certifique-se de que o sistema de arquivos ou grupo de discos exista e esteja disponível no host.

a. Clique em **Redefinir** para obter as configurações padrão dos parâmetros do banco de dados.

10. Na página PostOps, **Recuperar banco de dados** e **Até cancelar** são selecionados por padrão para executar a recuperação do banco de dados clonado.

    O SnapCenter executa a recuperação montando o backup de log mais recente que tem a sequência ininterrupta de logs de arquivamento após o backup de dados que foi selecionado para clonagem. O backup de log e dados deve estar no armazenamento primário para executar a clonagem no armazenamento primário e o backup de log e dados deve estar no armazenamento secundário para executar a clonagem no armazenamento secundário.

    As opções **Recuperar banco de dados** e **Até cancelar** não serão selecionadas se o SnapCenter não encontrar os backups de log apropriados. Você pode fornecer o local do log de arquivamento externo se o backup do log não estiver disponível em **Especificar locais do log de arquivamento externo**. Você pode especificar vários locais de log.

    Se você quiser clonar um banco de dados de origem configurado para oferecer suporte à área de recuperação flash (FRA) e ao Oracle Managed Files (OMF), o destino do log para recuperação também deverá aderir à estrutura de diretório do OMF.

    A página PostOps não será exibida se o banco de dados de origem for um banco de dados standby do Data Guard ou um banco de dados standby do Data Guard ativo. Para um banco de dados em espera do Data Guard ou um banco de dados em espera do Data Guard ativo, o SnapCenter não fornece uma opção para selecionar o tipo de recuperação na GUI do SnapCenter , mas o banco de dados é recuperado usando o tipo de recuperação Até Cancelar, sem aplicar nenhum log.

Nome do campo	Descrição
Até Cancelar	O SnapCenter executa a recuperação montando o backup de log mais recente com a sequência ininterrupta de logs de arquivo após o backup de dados que foi selecionado para clonagem. O banco de dados clonado é recuperado até o arquivo de log ausente ou corrompido.
Data e hora	O SnapCenter recupera o banco de dados até uma data e hora especificadas. O formato aceito é mm/dd/aaaa hh:mm:ss. O horário pode ser especificado no formato de 24 horas.
Até SCN (Número de Alteração do Sistema)	O SnapCenter recupera o banco de dados até um número de alteração do sistema (SCN) especificado.

Nome do campo	Descrição
Especificar locais de log de arquivo externo	Se o banco de dados estiver sendo executado no modo ARCHIVELOG, o SnapCenter identificará e montará o número ideal de backups de log com base no SCN especificado ou na data e hora selecionadas. Você também pode especificar o local do log de arquivamento externo. O SnapCenter não identificará nem montará automaticamente os backups de log se você tiver selecionado Até cancelar.
Criar novo DBID	Por padrão, a caixa de seleção **Criar novo DBID** é selecionada para gerar um número exclusivo (DBID) para o banco de dados clonado, diferenciando-o do banco de dados de origem. Desmarque a caixa de seleção se quiser atribuir o DBID do banco de dados de origem ao banco de dados clonado. Nesse cenário, se você quiser registrar o banco de dados clonado no catálogo RMAN externo onde o banco de dados de origem já está registrado, a operação falhará.
Criar arquivo temporário para espaço de tabela temporário	Marque a caixa de seleção se desejar criar um arquivo temporário para o tablespace temporário padrão do banco de dados clonado. Se a caixa de seleção não estiver marcada, o clone do banco de dados será criado sem o arquivo temporário.
Insira entradas SQL para aplicar quando o clone for criado	Adicione as entradas SQL que você deseja aplicar quando o clone for criado.

Nome do campo	Descrição
Insira scripts para executar após a operação de clonagem	Especifique o caminho e os argumentos do postscript que você deseja executar após a operação de clonagem. Você deve armazenar o postscript em */var/opt/snapcenter/spl/scripts* ou em qualquer pasta dentro deste caminho. Por padrão, o caminho */var/opt/snapcenter/spl/scripts* é preenchido. Se você colocou o script em qualquer pasta dentro deste caminho, você precisa fornecer o caminho completo até a pasta onde o script está colocado. Se a operação de clonagem falhar, os postscripts não serão executados e as atividades de limpeza serão acionadas diretamente.

11. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

    Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação de clonagem realizada, selecione **Anexar relatório de trabalho**.

    Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

12. Revise o resumo e clique em **Concluir**.

    Ao executar a recuperação como parte da operação de criação de clone, mesmo que a recuperação falhe, o clone será criado com um aviso. Você pode executar a recuperação manual neste clone para trazer o banco de dados clone para um estado consistente.

13. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Resultado

Após clonar o banco de dados, você pode atualizar a página de recursos para listar o banco de dados clonado como um dos recursos disponíveis para backup. O banco de dados clonado pode ser protegido como qualquer outro banco de dados usando o fluxo de trabalho de backup padrão ou pode ser incluído em um grupo de recursos (recém-criado ou existente). O banco de dados clonado pode ser clonado posteriormente (clone de clones).

Após a clonagem, você nunca deve renomear o banco de dados clonado.

Se você não tiver executado a recuperação durante a clonagem, o backup do banco de dados clonado poderá falhar devido à recuperação inadequada e talvez seja necessário executar a recuperação manual. O backup de log também pode falhar se o local padrão preenchido para logs de arquivamento estiver em um armazenamento que não seja da NetApp ou se o sistema de armazenamento não estiver configurado com o SnapCenter.

Na configuração do AIX, você pode usar o comando lkdev para bloquear e o comando rendev para renomear os discos nos quais o banco de dados clonado residia.

Bloquear ou renomear dispositivos não afetará a operação de exclusão de clones. Para layouts AIX LVM criados em dispositivos SAN, a renomeação de dispositivos não será suportada para os dispositivos SAN clonados.

Encontre mais informações

- "A restauração ou clonagem falha com a mensagem de erro ORA-00308"
- "Falha ao recuperar um banco de dados clonado"
- "Parâmetros personalizáveis para operações de backup, restauração e clonagem em sistemas AIX"

Atualizar o IP preferencial no host

Após a conclusão da operação de clonagem, o caminho fornecido pela Camada de Acesso ao Armazenamento (SAL) para o clone estará no formato *<nfs_lif_IP>:<JunctionPath>*. Para fornecer o IP preferencial, você deve configurá-lo no host usando os comandos SCCLI.

Passos

1. Efetue login no host do banco de dados.
2. Inicie uma sessão de conexão do PowerShell com o SnapCenter para um usuário especificado.

   Conexão Sm aberta

3. Crie um arquivo vazio.

   toque em /var/opt/snapcenter/scu/etc/storagepreference.properties

4. Configure o LIF de dados preferencial para o SVM.

   Add-SvmPreferredDataPath -SVM <Nome do SVM> -DataPath <endereço IP ou FQDN>

5. Verifique o caminho preferido.

   Obter-SvmPreferredDataPath

Clonar um banco de dados plugável

Você pode clonar um banco de dados conectável (PDB) para um CDB de destino diferente ou igual no mesmo host ou em um host alternativo. Você também pode recuperar o PDB clonado para um SCN ou data e hora desejados.

Antes de começar

Se você instalou o plug-in como um usuário não root, deverá atribuir manualmente as permissões de

execução aos diretórios prescript e postscript.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados do tipo instância única (multilocatário) na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

   A página de topologia do banco de dados é exibida.

4. Na exibição Gerenciar cópias, selecione os backups entre Cópias locais (primárias), Cópias espelhadas (secundárias) ou Cópias de cofre (secundárias).
5. Selecione o backup da tabela e clique em *  *.
6. Na página Nome, execute as seguintes ações:
   a. Selecione **PDB Clone**.
   b. Especifique o PDB que você deseja clonar.

      Você pode clonar apenas um PDB por vez.

   c. Especifique o nome do PDB clone.
7. Na página Locais, execute as seguintes ações:

Para este campo…	Faça isso…
Host clone	Por padrão, o host do banco de dados de origem é preenchido. Se você quiser criar o clone em um host alternativo, selecione o host que tenha a mesma versão do Oracle e do sistema operacional que o host do banco de dados de origem.
CDB alvo	Selecione o CDB onde você deseja incluir o PDB clonado. Você deve garantir que o CDB de destino esteja em execução.
Estado do banco de dados	Marque a caixa de seleção **Abrir o PDB clonado no modo LEITURA-GRAVAÇÃO** se desejar abrir o PDB no modo LEITURA-GRAVAÇÃO.

Localizações de arquivos de dados	Por padrão, o local do arquivo de dados é preenchido. A convenção de nomenclatura padrão do SnapCenter para sistemas de arquivos SAN ou NFS é FileSystemNameofsourcedatabase_SCJOBID. A convenção de nomenclatura padrão do SnapCenter para grupos de discos ASM é SC_HASHCODEofDISKGROUP_SCJOBID. O HASHCODEofDISKGROUP é um número gerado automaticamente (2 a 10 dígitos) que é exclusivo para cada grupo de discos ASM. Se você estiver personalizando o nome do grupo de discos ASM, certifique-se de que o comprimento do nome esteja de acordo com o comprimento máximo suportado pela Oracle. Se quiser especificar um caminho diferente, você deve inserir os pontos de montagem do arquivo de dados ou os nomes dos grupos de discos ASM para o banco de dados clone.

Os detalhes do Oracle home, nome de usuário e grupo são preenchidos automaticamente a partir do banco de dados de origem. Você pode alterar os valores com base no ambiente Oracle do host onde o clone será criado.

8. Na página PreOps, execute as seguintes etapas:

   a. Insira o caminho e os argumentos da prescrição que você deseja executar antes da operação de clonagem.

      Você deve armazenar a prescrição em /var/opt/snapcenter/spl/scripts ou em qualquer pasta dentro deste caminho. Por padrão, o caminho /var/opt/snapcenter/spl/scripts é preenchido. Se você colocou o script em qualquer pasta dentro deste caminho, você precisa fornecer o caminho completo até a pasta onde o script está colocado.

   O SnapCenter permite que você use as variáveis de ambiente predefinidas ao executar o prescript e o postscript."Saber mais"

   a. Na seção Configurações de parâmetros do banco de dados clone CDB auxiliar, modifique os valores dos parâmetros do banco de dados pré-preenchidos que são usados para inicializar o banco de dados.

9. Clique em **Redefinir** para obter as configurações padrão dos parâmetros do banco de dados.
10. Na página PostOps, **Até Cancelar** é selecionado por padrão para executar a recuperação do banco de dados clonado.

    A opção **Até Cancelar** não será selecionada se o SnapCenter não encontrar os backups de log

apropriados. Você pode fornecer o local do log de arquivamento externo se o backup do log não estiver disponível em **Especificar locais do log de arquivamento externo**. Você pode especificar vários locais de log.

Se você quiser clonar um banco de dados de origem configurado para oferecer suporte à área de recuperação flash (FRA) e ao Oracle Managed Files (OMF), o destino do log para recuperação também deverá aderir à estrutura de diretório do OMF.

Nome do campo	Descrição
Até Cancelar	O SnapCenter executa a recuperação montando o backup de log mais recente com a sequência ininterrupta de logs de arquivamento após o backup de dados que foi selecionado para clonagem. O backup de log e dados deve estar no armazenamento primário para executar a clonagem no armazenamento primário e o backup de log e dados deve estar no armazenamento secundário para executar a clonagem no armazenamento secundário. O banco de dados clonado é recuperado até o arquivo de log ausente ou corrompido.
Data e hora	O SnapCenter recupera o banco de dados até uma data e hora especificadas. O horário pode ser especificado no formato de 24 horas.
Até SCN (Número de Alteração do Sistema)	O SnapCenter recupera o banco de dados até um número de alteração do sistema (SCN) especificado.
Especificar locais de log de arquivo externo	Especifique o local do log de arquivamento externo.
Criar novo DBID	Por padrão, a caixa de seleção **Criar novo DBID** não está selecionada para o banco de dados clone auxiliar. Marque a caixa de seleção se desejar gerar um número exclusivo (DBID) para o banco de dados clonado auxiliar, diferenciando-o do banco de dados de origem.

Nome do campo	Descrição
Criar arquivo temporário para espaço de tabela temporário	Marque a caixa de seleção se desejar criar um arquivo temporário para o tablespace temporário padrão do banco de dados clonado. Se a caixa de seleção não estiver marcada, o clone do banco de dados será criado sem o arquivo temporário.
Insira entradas SQL para aplicar quando o clone for criado	Adicione as entradas SQL que você deseja aplicar quando o clone for criado.
Insira scripts para executar após a operação de clonagem	Especifique o caminho e os argumentos do postscript que você deseja executar após a operação de clonagem. Você deve armazenar o postscript em */var/opt/snapcenter/spl/scripts* ou em qualquer pasta dentro deste caminho. Por padrão, o caminho */var/opt/snapcenter/spl/scripts* é preenchido. Se você colocou o script em qualquer pasta dentro deste caminho, você precisa fornecer o caminho completo até a pasta onde o script está colocado. Se a operação de clonagem falhar, os postscripts não serão executados e as atividades de limpeza serão acionadas diretamente.

11. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

    Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação de clonagem realizada, selecione **Anexar relatório de trabalho**.

    Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

12. Revise o resumo e clique em **Concluir**.
13. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Depois que você terminar

Se você quiser criar um backup do PDB clonado, faça backup do CDB de destino onde o PDB foi clonado, porque não é possível fazer backup somente do PDB clonado. Você deve criar um relacionamento secundário para o CDB de destino se quiser criar o backup com relacionamento secundário.

Em uma configuração RAC, o armazenamento para PDB clonado é anexado somente ao nó onde o clone do

PDB foi executado. Os PDBs nos outros nós do RAC estão no estado MOUNT. Se quiser que o PDB clonado seja acessível a partir de outros nós, você deve anexar manualmente o armazenamento aos outros nós.

Encontre mais informações

- "A restauração ou clonagem falha com a mensagem de erro ORA-00308"
- "Parâmetros personalizáveis para operações de backup, restauração e clonagem em sistemas AIX"

Clonar backups de banco de dados Oracle usando comandos UNIX

O fluxo de trabalho do clone inclui o planejamento, a execução da operação de clone e o monitoramento da operação.

Sobre esta tarefa

Você deve executar os seguintes comandos para criar o arquivo de especificação de clone do banco de dados Oracle e iniciar a operação de clone.

As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando Get-Help *command_name*. Alternativamente, você também pode consultar o "Guia de referência de comandos do software SnapCenter" .

Passos

1. Crie uma especificação de clone do banco de dados Oracle a partir de um backup especificado: *New-SmOracleCloneSpecification*

   Se a política de proteção de dados secundária for unified mirror-vault, especifique somente -IncludeSecondaryDetails. Você não precisa especificar -SecondaryStorageType.

   Este comando cria automaticamente um arquivo de especificação de clone do banco de dados Oracle para o banco de dados de origem especificado e seu backup. Você também deve fornecer um SID de banco de dados clone para que o arquivo de especificação criado tenha os valores gerados automaticamente para o banco de dados clone que você criará.

   O arquivo de especificação do clone é criado em */var/opt/snapcenter/sco/clone_specs*.

2. Iniciar uma operação de clonagem de um grupo de recursos de clonagem ou de um backup existente: *New-SmClone*

   Este comando inicia uma operação de clonagem. Você também deve fornecer um caminho de arquivo de especificação de clone do Oracle para a operação de clone. Você também pode especificar as opções de recuperação, o host onde a operação de clonagem será realizada, prescrições, pós-escritos e outros detalhes.

   Por padrão, o arquivo de destino do log de arquivamento para o banco de dados clone é preenchido automaticamente em *$ORACLE_HOME/CLONE_SIDs*.

Dividir um clone do banco de dados Oracle

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido se torna independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clone em um clone intermediário.

  Por exemplo, depois de criar o clone1 a partir de um backup de banco de dados, você pode criar um backup do clone1 e então clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e você não pode executar a operação de divisão de clone no clone1. No entanto, você pode executar a operação de divisão de clone no clone2.

  Após dividir o clone2, você pode executar a operação de divisão do clone no clone1 porque o clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup do clone são excluídas.
- Para obter informações sobre as operações de divisão de volume do FlexClone , consultehttps://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html["Dividir um volume FlexClone de seu volume pai"]
- Certifique-se de que o volume ou agregado no sistema de armazenamento esteja online.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** na lista **Exibir**.
3. Selecione o recurso clonado (por exemplo, o banco de dados ou LUN) e clique em .
4. Revise o tamanho estimado do clone que será dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
5. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

   A operação de divisão de clones para de responder se o serviço SMCore for reiniciado e os bancos de dados nos quais a operação de divisão de clones foi executada forem listados como clones na página Recursos. Você deve executar o cmdlet *Stop-SmJob* para interromper a operação de divisão de clone e, em seguida, tentar novamente a operação de divisão de clone.

   Se você quiser um tempo de pesquisa maior ou menor para verificar se o clone está dividido ou não, você pode alterar o valor do parâmetro CloneSplitStatusCheckPollTime no arquivo SMCoreServiceHost.exe.config para definir o intervalo de tempo para o SMCore pesquisar o status da operação de divisão do clone. O valor está em milissegundos e o valor padrão é 5 minutos.

   Por exemplo,

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   A operação de início da divisão do clone falha se o backup, a restauração ou outra divisão do clone estiver em andamento. Você deve reiniciar a operação de divisão do clone somente após a conclusão das operações em execução.

Clone dividido de um banco de dados plugável

Você pode usar o SnapCenter para dividir um banco de dados plugável clonado (PDB).

Sobre esta tarefa

Se você criou um backup do CDB de destino onde o PDB foi clonado, quando você dividir o clone do PDB, o PDB clonado também será removido de todos os backups do CDB de destino que contém o PDB clonado.

Os clones do PDB não são exibidos na visualização de inventário ou recursos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Selecione o banco de dados do contêiner de origem (CDB) na exibição de recursos ou grupo de recursos.
3. Na exibição Gerenciar cópias, selecione **Clones** dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
4. Selecione o clone PDB (targetCDB:PDBClone) e clique em  .
5. Revise o tamanho estimado do clone que será dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Monitorar operações de clonagem do banco de dados Oracle

Você pode monitorar o progresso das operações de clonagem do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente operações de clonagem sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.

4. Selecione o trabalho de clonagem e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página Detalhes do trabalho, clique em **Exibir registros**.

Atualizar um clone

Você pode atualizar o clone executando o comando *Refresh-SmClone*. Este comando cria um backup do banco de dados, exclui o clone existente e cria um clone com o mesmo nome.

Não é possível atualizar um clone do PDB.

O que você vai precisar

- Crie um backup completo on-line ou uma política de backup de dados off-line sem backups agendados habilitados.
- Configure a notificação por e-mail na política somente para falhas de backup.
- Defina a contagem de retenção para os backups sob demanda adequadamente para garantir que não haja backups indesejados.
- Certifique-se de que somente um backup completo on-line ou uma política de backup de dados off-line esteja associada ao grupo de recursos identificado para a operação de atualização de clone.
- Crie um grupo de recursos com apenas um banco de dados.
- Se uma tarefa cron for criada para o comando clone refresh, certifique-se de que os agendamentos do SnapCenter e os agendamentos do cron não estejam sobrepostos para o grupo de recursos do banco de dados.

  Para uma tarefa cron criada para o comando clone refresh, certifique-se de executar o Open-SmConnection a cada 24 horas.

- Certifique-se de que o SID do clone seja exclusivo para um host.

  Se várias operações de atualização de clone usarem o mesmo arquivo de especificação de clone ou usarem o arquivo de especificação de clone com o mesmo SID de clone, o clone existente com o SID no host será excluído e então o clone será criado.

- Certifique-se de que a política de backup esteja habilitada com proteção secundária e que o arquivo de especificação do clone seja criado com “-IncludeSecondaryDetails” para criar os clones usando backups secundários.
  - Se o arquivo de especificação do clone primário for especificado, mas a política tiver a opção de atualização secundária selecionada, o backup será criado e a atualização será transferida para o secundário. No entanto, o clone será criado a partir do backup principal.
  - Se o arquivo de especificação do clone primário for especificado e a política não tiver a opção de atualização secundária selecionada, o backup será criado no primário e o clone será criado a partir do primário.

Passos

1. Iniciar uma sessão de conexão com o SnapCenter Server para um usuário especificado: *Open-SmConnection*
2. Crie uma especificação de clone do banco de dados Oracle a partir de um backup especificado: *New-*

SmOracleCloneSpecification

> Se a política de proteção de dados secundária for unified mirror-vault, especifique somente -IncludeSecondaryDetails. Você não precisa especificar -SecondaryStorageType.

Este comando cria automaticamente um arquivo de especificação de clone do banco de dados Oracle para o banco de dados de origem especificado e seu backup. Você também deve fornecer um SID de banco de dados clone para que o arquivo de especificação criado tenha os valores gerados automaticamente para o banco de dados clone que você criará.

> O arquivo de especificação do clone é criado em */var/opt/snapcenter/sco/clone_specs*.

3. Execute *Refresh-SmClone*.

   Se a operação falhar com as mensagens de erro "PL-SCO-20032: a operação canExecute falhou com o erro: PL-SCO-30031: o arquivo de log de refazer +SC_2959770772_clmdb/clmdb/redolog/redo01_01.log existe", especifique um valor mais alto para *-WaitToTriggerClone*.

   Para obter informações detalhadas sobre os comandos UNIX, consulte o "Guia de referência de comandos do software SnapCenter" .

Excluir clone de um banco de dados plugável

Você pode excluir o clone de um banco de dados conectável (PDB) se não precisar mais dele.

Se você criou um backup do CDB de destino onde o PDB foi clonado, quando você excluir o clone do PDB, o PDB clonado também será removido do backup do CDB de destino.

> Os clones do PDB não são exibidos na visualização de inventário ou recursos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Selecione o banco de dados do contêiner de origem (CDB) na exibição de recursos ou grupo de recursos.
3. Na exibição Gerenciar cópias, selecione **Clones** dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
4. Selecione o clone PDB (targetCDB:PDBClone) e clique em .
5. Clique em **OK**.

Gerenciar volumes de aplicativos

O que são volumes de aplicação

Os Volumes de Aplicativos são o armazenamento onde informações como configuração, instalador e outros arquivos não relacionados a dados relacionados ao banco de dados Oracle são armazenadas.

O plug-in SnapCenter para Oracle Database permite que você crie backups consistentes de volumes de

aplicativos (volumes não de dados) junto com os bancos de dados Oracle.

O plug-in automatiza o backup e a clonagem de volumes de aplicativos.

- Proteja volumes de aplicativos juntamente com volumes de banco de dados Oracle em um único grupo de recursos.
- Crie backups de volumes de aplicativos.
- Crie backups de bancos de dados Oracle junto com volumes de aplicativos.
- Crie clones de bancos de dados junto com volumes de aplicativos até um determinado momento.
- Agende operações de backup.
- Monitore todas as operações.
- Visualize relatórios de operações de backup e clonagem.

Adicionar volumes de aplicação

O SnapCenter oferece suporte ao backup e à clonagem de volumes de aplicativos do banco de dados Oracle. Você deve adicionar manualmente os volumes do aplicativo. A descoberta automática de volumes de aplicativos não é suportada.

Os volumes de aplicativos suportam apenas conexões NFS diretas e iSCSI diretas.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in do Oracle Database na lista.
2. Clique em **Adicionar volume do aplicativo**.
3. Na página Nome, execute as seguintes ações:
   - No campo Nome, insira o nome do volume do aplicativo.
   - No campo Nome do host, insira o nome do host.
4. Na página Storage Footprint, insira o nome do sistema de armazenamento, selecione um ou mais volumes e especifique os LUNs ou Qtrees associados.

   Você pode adicionar vários sistemas de armazenamento.

5. Revise o resumo e clique em **Concluir**.
6. Na página Recursos, selecione **Volume do aplicativo** na lista **Exibir** para visualizar todos os volumes de aplicativo que você adicionou.

Modificar volume do aplicativo

Você pode modificar todos os valores especificados ao adicionar o volume do aplicativo, se nenhum backup for criado. Se o backup for criado, você só poderá modificar os detalhes do sistema de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in do Oracle Database na lista.
2. Na página Recursos, selecione **Volume do aplicativo** na lista **Exibir**.
3.

Clique  para modificar os valores.

4. Clique  para modificar os valores.

Excluir volume do aplicativo

Quando você exclui um volume de aplicativo, se houver algum backup associado ao volume de aplicativo, o volume de aplicativo será colocado no modo de manutenção e nenhum novo backup será criado e nenhum backup anterior será retido. Se não houver backups associados, todos os metadados serão excluídos.

Se necessário, o SnapCenter permite que você desfaça a operação de exclusão.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in do Oracle Database na lista.
2. Na página Recursos, selecione **Volume do aplicativo** na lista **Exibir**.
3. Clique [elete icon] para modificar os valores.

Volumes de aplicativos de backup

Fazer backup do volume do aplicativo

Se o volume do aplicativo não fizer parte de nenhum grupo de recursos, você poderá fazer backup do volume do aplicativo na página Recursos.

Sobre esta tarefa

Por padrão, backups de grupo de consistência (CG) são criados. Se você quiser criar backups baseados em volume, defina o valor de **EnableOracleNdvVolumeBasedBackup** como true no arquivo *web.config*.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in do Oracle Database na lista.
2. Na página Recursos, selecione **Volume do aplicativo** na lista **Exibir**.
3. Clique *  * e selecione o nome do host e o tipo de banco de dados para filtrar os recursos.

   Você pode então clicar em *  * para fechar o painel de filtro.

4. Selecione o volume do aplicativo que você deseja fazer backup.

   A página Application volume-Protect é exibida.

5. Na página Recursos, execute as seguintes ações:

Para este campo…	Faça isso…
Use formato de nome personalizado para cópia do Snapshot	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot. Por exemplo, customtext__policy_hostname ou resource_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.
Excluir destinos de log de arquivo do backup	Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

6. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em * + *.

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

   c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

      policy_name é o nome da política que você selecionou.

   Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

7. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação de backup realizada no recurso, selecione **Anexar relatório de tarefa**.

   Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

8. Revise o resumo e clique em **Concluir**.

   A página de topologia de volume do aplicativo é exibida.

9. Clique em **Fazer backup agora**.
10. Na página Backup, execute as seguintes etapas:

    a. Se você aplicou várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

b. Clique em **Backup**.

11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Fazer backup do grupo de recursos de volumes do aplicativo

Você pode fazer backup do grupo de recursos que contém apenas volumes de aplicativos ou uma mistura de volumes de aplicativos e banco de dados. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos.

Se o grupo de recursos tiver vários volumes de aplicativo, todos os volumes de aplicativo deverão ter a política de replicação SnapMirror ou SnapVault .

Sobre esta tarefa

Por padrão, backups de grupo de consistência (CG) são criados. Se você quiser criar backups baseados em volume, defina o valor de **EnableOracleNdvVolumeBasedBackup** como true no arquivo *web.config*.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in do Oracle Database na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.

   Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou clicando em * * e, em seguida, selecionando a tag. Você pode então clicar em * * para fechar o painel de filtro.

3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e clique em **Fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
   a. Se você tiver associado várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

      Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

   b. Clique em **Backup**.
5. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

> A operação de verificação será realizada apenas para os bancos de dados e não para os volumes do aplicativo.

Clonar backup de volume do aplicativo

Você pode usar o SnapCenter para clonar os backups de volume do aplicativo.

Antes de começar

Se você instalou o plug-in como um usuário não root, deverá atribuir manualmente as permissões de

execução aos diretórios prescript e postscript.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in do Oracle Database na lista.
2. Na página Recursos, selecione **Volume do aplicativo** na lista **Exibir**.
3. Selecione o volume do aplicativo na exibição de detalhes do volume do aplicativo ou na exibição de detalhes do grupo de recursos.

   A página de topologia de volume do aplicativo é exibida.

4. Na exibição Gerenciar cópias, selecione os backups entre Cópias locais (primárias), Cópias espelhadas (secundárias) ou Cópias de cofre (secundárias).
5. Selecione o backup da tabela e clique em *  *.
6. Na página Localização, execute as seguintes ações:

Para este campo…	Faça isso…
Host de plug-in	Selecione o host onde você deseja criar o clone.
Nome do recurso de destino	Especifique o nome do recurso.

7. Na página Scripts, especifique os nomes dos scripts a serem executados antes da clonagem, os comandos para montar um sistema de arquivos e os nomes dos scripts a serem executados após a clonagem.
8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação de clonagem realizada, selecione **Anexar relatório de trabalho**.

   Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

9. Revise o resumo e clique em **Concluir**.

Dividir um clone de volume de aplicativo

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido se torna independente do recurso pai.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in do Oracle Database na lista.
2. Na página Recursos, selecione **Volume do aplicativo** na lista **Exibir**.
3. Selecione o recurso clonado e clique em  .
4. Revise o tamanho estimado do clone que será dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.

5. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Excluir um clone de volume de aplicativo

Você pode excluir clones se achar que eles não são mais necessários. Você não pode excluir clones que atuam como fonte para outros clones.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in do Oracle Database na lista.
2. Na página Recursos, selecione **Volume do aplicativo** na lista **Exibir**.
3. Selecione o recurso ou grupo de recursos na lista.

   A página de topologia do recurso ou do grupo de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Clones** dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
5. Selecione o clone e clique em  .
6. Na página Excluir clone, execute as seguintes ações:
   a. No campo **Pre clone delete**, insira os nomes dos scripts a serem executados antes de excluir o clone.
   b. No campo **Desmontar**, insira os comandos para desmontar o clone antes de excluí-lo.
7. Clique em **OK**.

Proteja os sistemas de arquivos do Windows

Conceitos do plug-in SnapCenter para Microsoft Windows

Visão geral do plug-in SnapCenter para Microsoft Windows

O SnapCenter Plug-in para Microsoft Windows é um componente do lado do host do NetApp SnapCenter Software que permite o gerenciamento de proteção de dados com reconhecimento de aplicativo dos recursos do sistema de arquivos da Microsoft. Além disso, ele fornece provisionamento de armazenamento, consistência de instantâneo e recuperação de espaço para sistemas de arquivos do Windows. O plug-in para Windows automatiza as operações de backup, restauração e clonagem do sistema de arquivos no seu ambiente SnapCenter .

Quando o plug-in para Windows estiver instalado, você poderá usar o SnapCenter com a tecnologia NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia NetApp SnapVault para executar a replicação de backup de disco para disco para arquivamento ou conformidade com padrões.

- Habilita a proteção de dados com reconhecimento de aplicativo para outros plug-ins que estão sendo executados em hosts Windows no seu ambiente SnapCenter
- Automatiza operações de backup, restauração e clonagem com reconhecimento de aplicativo para sistemas de arquivos Microsoft em seu ambiente SnapCenter
- Oferece suporte ao provisionamento de armazenamento, consistência de instantâneos e recuperação de espaço para hosts Windows

> O plug-in para Windows provisiona compartilhamentos SMB e sistemas de arquivos do Windows em LUNs físicos e RDM, mas não oferece suporte a operações de backup para sistemas de arquivos do Windows em compartilhamentos SMB.

O que você pode fazer com o plug-in SnapCenter para Microsoft Windows

Quando o Plug-in para Windows estiver instalado em seu ambiente, você poderá usar o SnapCenter para fazer backup, restaurar e clonar sistemas de arquivos do Windows. Você também pode executar tarefas de suporte a essas operações.

- Descubra recursos
- Fazer backup dos sistemas de arquivos do Windows
- Agendar operações de backup
- Restaurar backups do sistema de arquivos
- Backups do sistema de arquivos clone
- Monitore operações de backup, restauração e clonagem

> O plug-in para Windows não oferece suporte a backup e restauração de sistemas de arquivos em compartilhamentos SMB.

Recursos do plug-in SnapCenter para Windows

O plug-in para Windows integra-se à tecnologia NetApp Snapshot no sistema de armazenamento. Para trabalhar com o Plug-in para Windows, use a interface do SnapCenter .

O plug-in para Windows inclui estes recursos principais:

- **Interface gráfica de usuário unificada com tecnologia SnapCenter**

  A interface do SnapCenter oferece padronização e consistência entre plug-ins e ambientes. A interface do SnapCenter permite que você conclua processos consistentes de backup e restauração em todos os plug-ins, use relatórios centralizados, use visualizações de painel rápidas, configure o controle de acesso baseado em função (RBAC) e monitore trabalhos em todos os plug-ins. O SnapCenter também oferece agendamento centralizado e gerenciamento de políticas para dar suporte a operações de backup e clonagem.

- **Administração central automatizada**

  Você pode agendar backups de rotina do sistema de arquivos, configurar retenção de backup baseada em políticas e configurar operações de restauração. Você também pode monitorar proativamente o ambiente do seu sistema de arquivos configurando o SnapCenter para enviar alertas por e-mail.

- **Tecnologia NetApp Snapshot não disruptiva**

  O plug-in para Windows usa a tecnologia NetApp Snapshot. Isso permite que você faça backup de sistemas de arquivos em segundos e restaure-os rapidamente sem deixar o host offline. Os instantâneos consomem espaço de armazenamento mínimo.

Além desses recursos principais, o Plug-in para Windows oferece os seguintes benefícios:

- Suporte para fluxo de trabalho de backup, restauração e clonagem
- Segurança com suporte RBAC e delegação centralizada de funções
- Criação de cópias com eficiência de espaço de sistemas de arquivos de produção para testes ou extração de dados usando a tecnologia NetApp FlexClone

  Para obter informações sobre o licenciamento do FlexClone , consulte"Licenças SnapCenter" .

- Capacidade de executar vários backups ao mesmo tempo em vários servidores
- Cmdlets do PowerShell para scripts de operações de backup, restauração e clonagem
- Suporte para backup de sistemas de arquivos e discos de máquinas virtuais (VMDKs)
- Suporte para infraestruturas físicas e virtualizadas
- Suporte para iSCSI, Fibre Channel, FCoE, mapeamento de dispositivos brutos (RDM), mapeamento de LUN assimétrico (ALM), VMDK sobre NFS e VMFS e FC virtual
- Suporte para memória não volátil expressa (NVMe) no Windows Server 2022
  - Fluxos de trabalho de backup, restauração, clonagem e verificação no layout VMDK criado em NVMe sobre TCP/IP.
  - Suporta firmware NVMe versão 1.3 a partir do ESX 8.0 atualização 2 e requer hardware virtual versão 21.

    - O Windows Server Failover Clustering (WSFC) não é suportado para aplicativos via VMDK em NVMe via TCP/IP.
- Oferece suporte à sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC]), que permite que os serviços empresariais continuem operando mesmo durante uma falha completa do site, permitindo que os aplicativos façam failover de forma transparente usando uma cópia secundária. Não é necessária intervenção manual nem script adicional para acionar um failover com a sincronização ativa do SnapMirror .

Como o SnapCenter faz backup dos sistemas de arquivos do Windows

O SnapCenter usa a tecnologia Snapshot para fazer backup de recursos do sistema de arquivos do Windows que residem em LUNs, CSVs (volumes compartilhados de cluster), volumes RDM (mapeamento de dispositivos brutos), ALM (mapeamento de LUN assimétrico) em clusters do Windows e VMDKs baseados em VMFS/NFS (VMware Virtual Machine File System usando NFS).

O SnapCenter cria backups criando instantâneos dos sistemas de arquivos. Backups federados, nos quais um volume contém LUNs de vários hosts, são mais rápidos e eficientes do que backups de cada LUN individual porque apenas um Snapshot do volume é criado em comparação com Snapshots individuais de cada sistema de arquivos.

Quando o SnapCenter cria um Snapshot, todo o volume do sistema de armazenamento é capturado no Snapshot. No entanto, o backup é válido somente para o servidor host para o qual o backup foi criado.

Se houver dados de outros servidores host no mesmo volume, esses dados não poderão ser restaurados do Snapshot.

Se um sistema de arquivos do Windows contiver um banco de dados, fazer backup do sistema de arquivos não será o mesmo que fazer backup do banco de dados. Para fazer backup de um banco de dados, você deve usar um dos plug-ins de banco de dados.

Tipos de armazenamento suportados pelo SnapCenter Plug-in para Microsoft Windows

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e virtuais. Você deve verificar se o suporte está disponível para seu tipo de armazenamento antes de instalar o pacote para seu host.

O suporte ao provisionamento e à proteção de dados do SnapCenter está disponível no Windows Server. Para obter as informações mais recentes sobre as versões suportadas, consulte ohttps://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT["Ferramenta de Matriz de Interoperabilidade da NetApp"^] .

Máquina	Tipo de armazenamento	Provisão usando	Notas de suporte
Servidor físico	LUNs conectados por FC	Interface gráfica do usuário (GUI) do SnapCenter ou cmdlets do PowerShell	

Máquina	Tipo de armazenamento	Provisão usando	Notas de suporte
Servidor físico	LUNs conectados por iSCSI	Cmdlets do SnapCenter GUI ou PowerShell	
Servidor físico	Compartilhamentos SMB3 (CIFS) residindo em uma máquina virtual de armazenamento (SVM)	Cmdlets do SnapCenter GUI ou PowerShell	Suporte somente para provisionamento.
VMware VM	LUNs RDM conectados por um FC ou iSCSI HBA	Cmdlets do PowerShell	
VMware VM	LUNs iSCSI conectados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets do SnapCenter GUI ou PowerShell	
VMware VM	Sistemas de arquivos de máquina virtual (VMFS) ou armazenamentos de dados NFS	VMware vSphere	
VMware VM	Um sistema convidado conectado a compartilhamentos SMB3 que residem em um SVM	Cmdlets do SnapCenter GUI ou PowerShell	Suporte somente para provisionamento.
VMware VM	Armazenamentos de dados vVol em NFS e SAN	Ferramentas ONTAP para VMware vSphere	

Máquina	Tipo de armazenamento	Provisão usando	Notas de suporte
VM Hyper-V	LUNs FC virtuais (vFC) conectados por um switch Fibre Channel virtual	Cmdlets do SnapCenter GUI ou PowerShell	Você deve usar o Hyper-V Manager para provisionar LUNs de FC Virtual (vFC) conectados por um Switch de Canal de Fibra virtual. Não há suporte para discos de passagem do Hyper-V e backup de bancos de dados em VHD(x) provisionados no armazenamento NetApp .
VM Hyper-V	LUNs iSCSI conectados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets do SnapCenter GUI ou PowerShell	Não há suporte para discos de passagem do Hyper-V e backup de bancos de dados em VHD(x) provisionados no armazenamento NetApp .

Máquina	Tipo de armazenamento	Provisão usando	Notas de suporte
VM Hyper-V	Um sistema convidado conectado a compartilhamentos SMB3 que residem em um SVM	Cmdlets do SnapCenter GUI ou PowerShell	Suporte somente para provisionamento. Não há suporte para discos de passagem do Hyper-V e backup de bancos de dados em VHD(x) provisionados no armazenamento NetApp .

Privilégios ONTAP mínimos necessários para o plug-in do Windows

Os privilégios mínimos do ONTAP necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos de acesso total: privilégios mínimos necessários para ONTAP 9.12.1 e posterior
  - evento generate-autosupport-log
  - histórico de trabalho mostrar
  - parada de trabalho
  - lua
  - lun criar
  - lun delete
  - lun igroup adicionar
  - lun igroup criar
  - lun igroup excluir
  - renomear lun igroup
  - show do lun igroup
  - mapeamento lun add-reporting-nodes
  - criação de mapeamento lun
  - exclusão de mapeamento lun
  - mapeamento lun remove-reporting-nodes
  - show de mapeamento lunar
  - lun modificar

- volume de entrada lun
- lua offline
- lua online
- redimensionamento de lun
- série lun
- show de lua
- política de adição de regra do snapmirror
- regra de modificação de política do snapmirror
- política de remoção do snapmirror
- política do snapmirror mostrar
- restauração do snapmirror
- show de espelhos instantâneos
- histórico de exibição do snapmirror
- atualização do snapmirror
- atualização do snapmirror-ls-set
- lista-destinos do snapmirror
- versão
- criação de clone de volume
- show de clones de volume
- volume clone split start
- volume clone divisão parada
- volume criar
- destruição de volume
- clone de arquivo de volume criar
- arquivo de volume mostrar-uso-do-disco
- volume offline
- volume on-line
- modificação de volume
- volume qtree criar
- volume qtree delete
- volume qtree modificar
- volume qtree mostrar
- restrição de volume
- show de volume
- criação de instantâneo de volume
- exclusão de instantâneo de volume
- modificação de instantâneo de volume

    - renomeação de instantâneo de volume
    - restauração de instantâneo de volume
    - arquivo de restauração de instantâneo de volume
    - exibição de instantâneo de volume
    - desmontagem de volume
    - cifs do vserver
    - vserver cifs compartilhar criar
    - vserver cifs compartilhar excluir
    - vserver cifs shadowcopy mostrar
    - vserver cifs compartilhar mostrar
    - vserver cifs mostrar
    - política de exportação do vserver
    - criação de política de exportação do vserver
    - exclusão da política de exportação do vserver
    - criação de regra de política de exportação do vserver
    - mostrar regra de política de exportação do vserver
    - mostrar política de exportação do vserver
    - vserver iscsi
    - mostrar conexão iscsi do vserver
    - vserver mostrar
- Comandos somente leitura: privilégios mínimos necessários para ONTAP 8.3.0 e posterior
    - interface de rede
    - exibição de interface de rede
    - vserver

Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault

Você pode usar um plug-in SnapCenter com a tecnologia ONTAP SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia ONTAP SnapVault para executar replicação de backup de disco para disco para conformidade com padrões e outros propósitos relacionados à governança. Antes de executar essas tarefas, você deve configurar um relacionamento de proteção de dados entre os volumes de origem e destino e inicializar o relacionamento.

O SnapCenter executa as atualizações no SnapMirror e no SnapVault após concluir a operação Snapshot. As atualizações do SnapMirror e do SnapVault são executadas como parte do trabalho do SnapCenter ; não crie uma programação ONTAP separada.

Se você estiver acessando o SnapCenter a partir de um produto NetApp SnapManager e estiver satisfeito com os relacionamentos de proteção de dados configurados, pode pular esta seção.

Um relacionamento de proteção de dados replica dados do armazenamento primário (o volume de origem) para o armazenamento secundário (o volume de destino). Quando você inicializa o relacionamento, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não oferece suporte a relacionamentos em cascata entre volumes SnapMirror e SnapVault (**Primário** > **Espelho** > **Cofre**). Você deve usar relacionamentos fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis em termos de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis em termos de versão e como configurá-los, consulte "Documentação do ONTAP" .

Definir uma estratégia de backup para sistemas de arquivos do Windows

Definir uma estratégia de backup antes de criar seus backups fornece os backups necessários para restaurar ou clonar seus sistemas de arquivos com sucesso. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (RTO) e objetivo de ponto de recuperação (RPO) determinam em grande parte sua estratégia de backup.

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. RTO é o tempo em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. SLA, RTO e RPO contribuem para a estratégia de proteção de dados.

Agendamentos de backup para sistemas de arquivos do Windows

A frequência de backup é especificada nas políticas; um agendamento de backup é especificado na configuração do grupo de recursos. O fator mais crítico na determinação da frequência ou programação de backup é a taxa de alteração do recurso e a importância dos dados. Você pode fazer backup de um recurso muito utilizado a cada hora, enquanto pode fazer backup de um recurso raramente utilizado uma vez por dia. Outros fatores incluem a importância do recurso para sua organização, seu Acordo de Nível de Serviço (SLA) e seu Objetivo de Ponto de Recuperação (RPO).

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. Um RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. O SLA e o RPO contribuem para a estratégia de proteção de dados.

Mesmo para um recurso muito utilizado, não há necessidade de executar um backup completo mais de uma ou duas vezes por dia.

Os agendamentos de backup têm duas partes, conforme a seguir:

- Frequência de backup

  A frequência de backup (com que frequência os backups devem ser realizados), chamada de *tipo de agendamento* para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como horária, diária, semanal ou mensal, ou pode especificar **Nenhum**, o que torna a política somente sob demanda. Você pode acessar as políticas clicando em **Configurações** > **Políticas**.

- Agendamentos de backup

Os agendamentos de backup (exatamente quando os backups devem ser executados) fazem parte de uma configuração de grupo de recursos. Por exemplo, se você tiver um grupo de recursos com uma política configurada para backups semanais, poderá configurar o agendamento para fazer backup toda quinta-feira às 22h. Você pode acessar as programações dos grupos de recursos clicando em **Recursos** > **Grupos de Recursos**.

Número de backups necessários para sistemas de arquivos do Windows

Os fatores que determinam o número de backups necessários incluem o tamanho do sistema de arquivos do Windows, o número de volumes usados, a taxa de alteração do sistema de arquivos e seu Contrato de Nível de Serviço (SLA).

Convenção de nomenclatura de backup para sistemas de arquivos do Windows

Os backups do sistema de arquivos do Windows usam a convenção de nomenclatura Snapshot padrão. A convenção de nomenclatura de backup padrão adiciona um registro de data e hora aos nomes de instantâneos que ajuda a identificar quando as cópias foram criadas.

O Snapshot usa a seguinte convenção de nomenclatura padrão: resourcegroupname_hostname_timestamp

Você deve nomear seus grupos de recursos de backup logicamente, como no exemplo a seguir:

```
dts1_mach1x88_03-12-2015_23.17.26
```

Neste exemplo, os elementos de sintaxe têm os seguintes significados:

- `dts1`é o nome do grupo de recursos.
- `mach1x88`é o nome do host.
- `03-12-2016_23.17.26`é a data e o carimbo de data/hora.

Ao criar um backup, você também pode adicionar uma tag descritiva para ajudar a identificar o backup. Por outro lado, se você quiser usar uma convenção de nomenclatura de backup personalizada, precisará renomear o backup após a conclusão da operação de backup.

Opções de retenção de backup

Você pode escolher o número de dias pelos quais deseja manter cópias de backup ou especificar o número de cópias de backup que deseja manter, até um máximo ONTAP de 255 cópias. Por exemplo, sua organização pode exigir que você mantenha 10 dias de cópias de backup ou 130 cópias de backup.

Ao criar uma política, você pode especificar as opções de retenção para o tipo de backup e o tipo de agendamento.

Se você configurar a replicação do SnapMirror , a política de retenção será espelhada no volume de destino.

O SnapCenter exclui os backups retidos que têm rótulos de retenção que correspondem ao tipo de agendamento. Se o tipo de agendamento foi alterado para o recurso ou grupo de recursos, os backups com o rótulo de tipo de agendamento antigo ainda poderão permanecer no sistema.

Para retenção de cópias de backup a longo prazo, você deve usar o backup SnapVault .

Origens e destinos de clones para sistemas de arquivos do Windows

Você pode clonar um backup do sistema de arquivos do armazenamento primário ou secundário. Você também pode escolher o destino que atende às suas necessidades: o local de backup original ou um destino diferente no mesmo host ou em um host diferente. O destino deve estar no mesmo volume que o backup de origem do clone.

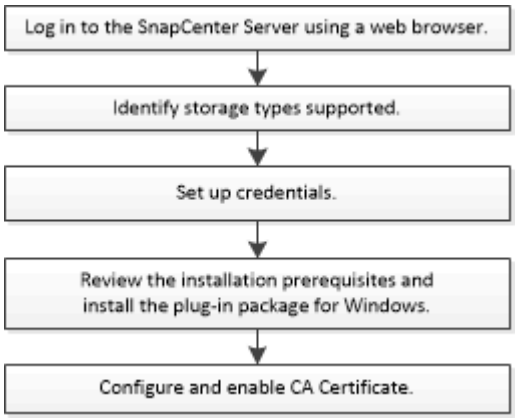
Destino do clone	Descrição
Original, fonte, localização	Por padrão, o SnapCenter armazena o clone no mesmo local e no mesmo host que o backup que está sendo clonado.
Localização diferente	Você pode armazenar o clone em um local diferente no mesmo host ou em um host diferente. O host deve ter uma conexão configurada com a máquina virtual de armazenamento (SVM).

Você pode renomear o clone após a conclusão da operação de clonagem.

Instalar o plug-in SnapCenter para Microsoft Windows

Fluxo de trabalho de instalação do plug-in SnapCenter para Microsoft Windows

Você deve instalar e configurar o SnapCenter Plug-in para Microsoft Windows se quiser proteger arquivos do Windows que não sejam arquivos de banco de dados.



Requisitos de instalação do plug-in SnapCenter para Microsoft Windows

Você deve estar ciente de certos requisitos de instalação antes de instalar o Plug-in para Windows.

Antes de começar a usar o Plug-in para Windows, o administrador do SnapCenter deve instalar e configurar o SnapCenter Server e executar tarefas de pré-requisito.

- Você precisa ter privilégios de administrador do SnapCenter para instalar o Plug-in para Windows.

A função de administrador do SnapCenter deve ter privilégios de administrador.

- Você deve ter instalado e configurado o SnapCenter Server.
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.
- Você deve configurar o SnapMirror e o SnapVault se quiser replicação de backup.

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows

Antes de instalar o pacote de plug-ins do SnapCenter para Windows, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas Operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Se você estiver em uma configuração de cluster do Windows, também deverá instalar e configurar o Gerenciamento Remoto do Windows (WinRM).
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	5 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.

Item	Requisitos
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell Core 7.4.2 Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."

Configure suas credenciais para o Plug-in para Windows

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter . Você deve criar credenciais para instalar plug-ins do SnapCenter e credenciais adicionais para executar operações de proteção de dados em sistemas de arquivos do Windows.

O que você vai precisar

- Você deve configurar as credenciais do Windows antes de instalar plug-ins.
- Você deve configurar as credenciais com privilégios de administrador, incluindo direitos de administrador, no host remoto.
- Se você configurar credenciais para grupos de recursos individuais e o usuário não tiver privilégios de administrador completos, será necessário atribuir pelo menos os privilégios de grupo de recursos e backup ao usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.
4. Na página Credencial, faça o seguinte:

Para este campo…	Faça isso…
Nome da credencial	Digite um nome para as credenciais.

Para este campo…	Faça isso…
Nome de usuário/Senha	Digite o nome de usuário e a senha usados para autenticação. • Administrador de domínio ou qualquer membro do grupo de administradores Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são os seguintes: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • Administrador local (somente para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é o seguinte: `UserName` Não use aspas duplas (") ou acento grave (`) nas senhas. Você não deve usar os símbolos de menor que (<) e exclamação (!) juntos em senhas. Por exemplo, menor que <! 10, menor que 10 <!, acento grave `12.
Senha	Digite a senha usada para autenticação.

5. Clique em **OK**.

   Depois de concluir a configuração das credenciais, talvez você queira atribuir a manutenção de credenciais a um usuário ou grupo de usuários na página Usuário e Acesso.

Configurar o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite que você crie uma Conta de Serviço Gerenciada de grupo (gMSA) que fornece gerenciamento automatizado de senhas de contas de serviço a partir de uma conta de domínio gerenciada.

Antes de começar

- Você deve ter um controlador de domínio do Windows Server 2016 ou posterior.
- Você deve ter um host Windows Server 2016 ou posterior, que seja membro do domínio.

Passos

1. Crie uma chave raiz do KDS para gerar senhas exclusivas para cada objeto no seu gMSA.
2. Para cada domínio, execute o seguinte comando no controlador de domínio do Windows: Add-KDSRootKey -EffectiveImmediately
3. Crie e configure seu gMSA:
   a. Crie uma conta de grupo de usuários no seguinte formato:

```
 domainName\accountName$
.. Adicione objetos de computador ao grupo.
.. Use o grupo de usuários que você acabou de criar para criar o
gMSA.
```

   Por exemplo,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correr `Get-ADServiceAccount` comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Habilite o módulo do Active Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando no PowerShell:

```
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. Reinicie seu host.

b. Instale o gMSA no seu host executando o seguinte comando no prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua privilégios administrativos ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no SnapCenter Server.

   O SnapCenter Server instalará os plug-ins selecionados no host e o gMSA especificado será usado como a conta de logon de serviço durante a instalação do plug-in.

Adicionar hosts e instalar o plug-in SnapCenter para Microsoft Windows

Você pode usar a página Adicionar Host do SnapCenter para adicionar hosts do Windows. O plug-in SnapCenter para Microsoft Windows é instalado automaticamente no host especificado. Este é o método recomendado para instalar plug-ins. Você pode adicionar um host e instalar um plug-in para um host individual ou um cluster.

Antes de começar

- Se o sistema operacional do host do SnapCenter Server for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deverá executar o seguinte:
  - Atualize para o Windows Server 2019 (versão do sistema operacional 17763.5936) ou posterior
  - Atualize para o Windows Server 2022 (versão do sistema operacional 20348.2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.

- O usuário do SnapCenter deve ser adicionado à função “Fazer logon como um serviço” do Windows Server.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- Se estiver usando uma conta de serviço gerenciada em grupo (gMSA), você deverá configurar a gMSA com privilégios administrativos.

  "Configurar conta de serviço gerenciada de grupo no Windows Server 2016 ou posterior para o sistema de arquivos do Windows"

Sobre esta tarefa

- Não é possível adicionar um SnapCenter Server como um host de plug-in a outro SnapCenter Server.
- Plug-ins do Windows
  - Microsoft Windows
  - Servidor Microsoft Exchange
  - Servidor Microsoft SQL
  - SAP HANA
- Instalando plug-ins em um cluster

  Se você instalar plug-ins em um cluster (WSFC, Oracle RAC ou Exchange DAG), eles serão instalados em todos os nós do cluster.

- Armazenamento da série E

  Não é possível instalar o Plug-in para Windows em um host Windows conectado ao armazenamento da série E.

> O SnapCenter não oferece suporte à adição do mesmo host (host de plug-in) ao SnapCenter se o host já fizer parte de um grupo de trabalho e tiver sido alterado para outro domínio ou vice-versa. Se quiser adicionar o mesmo host, você deve removê-lo do SnapCenter e adicioná-lo novamente.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Certifique-se de que **Hosts gerenciados** esteja selecionado na parte superior.
3. Clique em **Adicionar**.
4. Na página Hosts, faça o seguinte:

Para este campo…	Faça isso…
Tipo de host	Selecione o tipo de host **Windows**. O SnapCenter Server adiciona o host e instala o Plug-in para Windows, caso ele ainda não esteja instalado no host.

Para este campo…	Faça isso…
Nome do host	Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o nome de domínio totalmente qualificado (FQDN). Você pode inserir os endereços IP ou FQDN de um dos seguintes: • Host autônomo • Cluster de Failover do Windows Server (WSFC) Se você estiver adicionando um host usando o SnapCenter e ele fizer parte de um subdomínio, você deverá fornecer o FQDN.
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte informações sobre como criar uma credencial. Detalhes sobre credenciais, incluindo nome de usuário, domínio e tipo de host, são exibidos colocando o cursor sobre o nome da credencial fornecido. O modo de autenticação é determinado pelo tipo de host especificado no assistente Adicionar Host.

5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a serem instalados.

   Para novas implantações, nenhum pacote de plug-in é listado.

6. (Opcional) Clique em **Mais opções**.

Para este campo…	Faça isso…
Porta	Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.
Caminho de instalação	O caminho padrão é C:\Arquivos de Programas\ NetApp\ SnapCenter. Opcionalmente, você pode personalizar o caminho. Para o pacote de plug-ins SnapCenter para Windows, o caminho padrão é C:\Arquivos de Programas\ NetApp\ SnapCenter. No entanto, se desejar, você pode personalizar o caminho padrão.
Adicionar todos os hosts no cluster	Marque esta caixa de seleção para adicionar todos os nós do cluster em um WSFC.
Ignorar verificações de pré-instalação	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.
Use a conta de serviço gerenciada em grupo (gMSA) para executar os serviços do plug-in	Marque esta caixa de seleção se desejar usar a Conta de Serviço Gerenciada em Grupo (gMSA) para executar os serviços do plug-in. Forneça o nome do gMSA no seguinte formato: *domainName\accountName$*. O gMSA será usado como uma conta de serviço de logon somente para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

Se você não tiver marcado a caixa de seleção **Ignorar pré-verificações**, o host será validado para verificar se atende aos requisitos para instalar o plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão do .NET e a localização são validados em relação aos requisitos mínimos. Se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas serão exibidas.

Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em `C:\Program Files\NetApp\SnapCenter` WebApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.

> Em uma configuração de HA, se você estiver atualizando o arquivo web.config, deverá atualizar o arquivo em ambos os nós.

8. Monitore o progresso da instalação.

Instalar o plug-in SnapCenter para Microsoft Windows em vários hosts remotos usando cmdlets do PowerShell

Se você deseja instalar o SnapCenter Plug-in para Microsoft Windows em vários hosts ao mesmo tempo, você pode fazer isso usando o `Install-SmHostPackage` Cmdlet do PowerShell.

Você deve ter efetuado login no SnapCenter como um usuário de domínio com direitos de administrador local em cada host no qual deseja instalar plug-ins.

Passos

1. Inicie o PowerShell.
2. No host do SnapCenter Server, estabeleça uma sessão usando o `Open-SmConnection` cmdlet e insira suas credenciais.
3. Adicione o host autônomo ou o cluster ao SnapCenter usando o `Add-SmHost` cmdlet e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

4. Instale o plug-in em vários hosts usando o `Install-SmHostPackage` cmdlet e os parâmetros necessários.

   Você pode usar o `-skipprecheck` opção quando você instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.

Instale o plug-in SnapCenter para Microsoft Windows silenciosamente a partir da linha de comando

Você pode instalar o SnapCenter Plug-in para Microsoft Windows localmente em um host Windows se não conseguir instalar o plug-in remotamente a partir da GUI do SnapCenter . Você pode executar o programa de instalação do SnapCenter Plug-in para Microsoft Windows sem supervisão, no modo silencioso, a partir da linha de comando do Windows.

Antes de começar

- Você deve ter instalado o ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) Hosting Bundle.
- Você deve ter instalado o PowerShell 7.4.2 ou posterior.

- Você deve ser um administrador local no host.

Passos

1. Baixe o plug-in SnapCenter para Microsoft Windows do seu local de instalação.

   Por exemplo, o caminho de instalação padrão é C:\ProgramData\ NetApp\ SnapCenter\Package Repository.

   Este caminho pode ser acessado a partir do host onde o SnapCenter Server está instalado.

2. Copie o arquivo de instalação para o host no qual você deseja instalar o plug-in.
3. No prompt de comando, navegue até o diretório onde você baixou o arquivo de instalação.
4. Digite o seguinte comando, substituindo as variáveis pelos seus dados:

   ```
   "snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
   BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
   ISFeatureInstall=SCW
   ```

   Por exemplo:

   ```
   `"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`
   ```

   Todos os parâmetros passados durante a instalação do Plug-in para Windows diferenciam maiúsculas de minúsculas.

   Insira os valores para as seguintes variáveis:

Variável	Valor
/debuglog"<Caminho_do_Log_de_Depuração>	Especifique o nome e o local do arquivo de log do instalador do pacote, como no exemplo a seguir: Setup.exe /debuglog"C:\PathToLog\setupexe.log".
PORTA_BI_SNAPCENTER	Especifique a porta na qual o SnapCenter se comunica com o SMCore.
SUITE_INSTALLDIR	Especifique o diretório de instalação do pacote de plug-in do host.
CONTA_DE_SERVIÇO_BI	Especifique o plug-in SnapCenter para a conta de serviço web do Microsoft Windows.

Variável	Valor
BI_SERVICEPWD	Especifique a senha para a conta de serviço web do SnapCenter Plug-in para Microsoft Windows.
Instalação do ISFeature	Especifique a solução a ser implantada pelo SnapCenter no host remoto.

O parâmetro *debuglog* inclui o caminho do arquivo de log do SnapCenter. Gravar neste arquivo de log é o método preferencial para obter informações de solução de problemas, porque o arquivo contém os resultados das verificações que a instalação executa para pré-requisitos de plug-in.

Se necessário, você pode encontrar informações adicionais sobre solução de problemas no arquivo de log do pacote SnapCenter para Windows. Os arquivos de log do pacote são listados (os mais antigos primeiro) na pasta *%Temp%*, por exemplo, *C:\temp*.

A instalação do Plug-in para Windows registra o plug-in no host e não no SnapCenter Server. Você pode registrar o plug-in no SnapCenter Server adicionando o host usando a GUI do SnapCenter ou o cmdlet do PowerShell. Depois que o host é adicionado, o plug-in é descoberto automaticamente.

Monitorar o status de instalação do pacote de plug-in SnapCenter

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
   a. Clique em **Filtrar**.
   b. Opcional: especifique a data de início e término.
   c. No menu suspenso Tipo, selecione **Instalação de plug-in**.

d. No menu suspenso Status, selecione o status da instalação.

e. Clique em **Aplicar**.

4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Configurar certificado CA

Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.

O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte "Como gerar um arquivo CSR de certificado CA" .

Se você possui o certificado CA para seu domínio (*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Importar chave privada	Selecione a opção **Sim**, importe a chave privada e clique em **Avançar**.
Formato de arquivo de importação	Não faça alterações; clique em **Avançar**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: *.pfx, *.p12 e *.p7b).

7. Repita a Etapa 5 para a pasta “Pessoal”.

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

Passos

1. Execute o seguinte na GUI:
   a. Clique duas vezes no certificado.
   b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.
   c. Percorra a lista de campos e clique em **Impressão digital**.
   d. Copie os caracteres hexadecimais da caixa.
   e. Remova os espaços entre os números hexadecimais.

      Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
   a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copie a impressão digital.

Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Por exemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Vincule o certificado recém-instalado aos serviços de plug-in do host
   do Windows, executando os seguintes comandos:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Por exemplo:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *Get-SmCertificateSettings*.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.

3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- * * indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- * * indica que o certificado CA foi validado com sucesso.
- * * indica que o certificado CA não pôde ser validado.
- * * indica que as informações de conexão não puderam ser recuperadas.

Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Instalar o SnapCenter Plug-in for VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs), ou se você quiser proteger VMs e armazenamentos de dados, será necessário implantar o SnapCenter Plug-in for VMware vSphere .

Para obter informações sobre como implantar, consulte "Visão geral da implantação" .

Implantar certificado CA

Para configurar o Certificado CA com o SnapCenter Plug-in for VMware vSphere, consulte "Criar ou importar certificado SSL" .

Configurar o arquivo CRL

O SnapCenter Plug-in for VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL do SnapCenter Plug-in for VMware vSphere é */opt/netapp/config/crl*.

Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

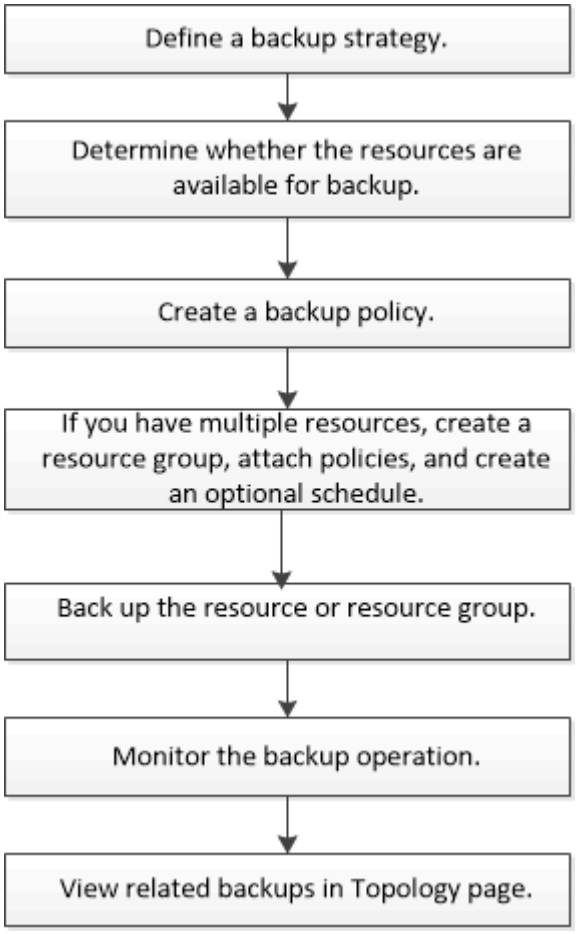
Fazer backup dos sistemas de arquivos do Windows

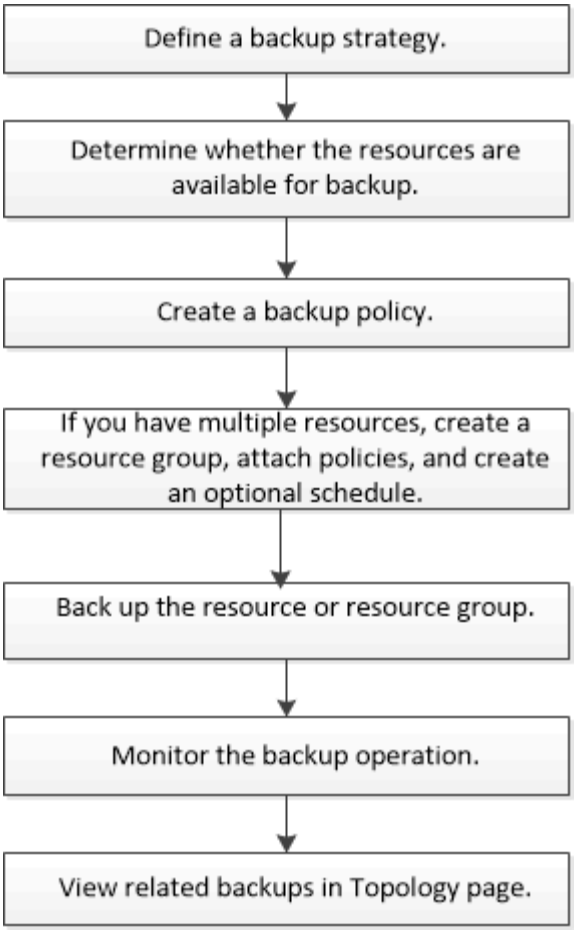
Fazer backup dos sistemas de arquivos do Windows

Ao instalar o SnapCenter Plug-in para Microsoft Windows em seu ambiente, você pode usar o SnapCenter para fazer backup dos sistemas de arquivos do Windows. Você pode fazer backup de um único sistema de arquivos ou de um grupo de recursos que contém vários sistemas de arquivos. Você pode fazer backup sob demanda ou de acordo com um cronograma de proteção definido.

Você pode agendar vários backups para serem executados em todos os servidores simultaneamente. As operações de backup e restauração não podem ser executadas simultaneamente no mesmo recurso.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar as operações de backup:





Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter ou o "Guia de referência do cmdlet do software SnapCenter" contém informações detalhadas sobre cmdlets do PowerShell.

Determinar a disponibilidade de recursos para sistemas de arquivos do Windows

Recursos são LUNs e componentes semelhantes no seu sistema de arquivos que são mantidos pelos plug-ins que você instalou. Você pode adicionar esses recursos a grupos de recursos para poder executar tarefas de proteção de dados em vários recursos, mas primeiro você deve identificar quais recursos estão disponíveis. Descobrir os recursos disponíveis também verifica se a instalação do plug-in foi concluída com sucesso.

Antes de começar

- Você já deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts, criar conexões de máquina virtual de armazenamento (SVM) e adicionar credenciais.
- Se os arquivos residirem em LUNs ou VMDKs do VMware RDM, você deverá implantar o SnapCenter Plug-in for VMware vSphere e registrar o plug-in no SnapCenter. Para obter mais informações, consulte "Documentação do SnapCenter Plug-in for VMware vSphere" .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Sistemas de arquivos** na lista.
3. Selecione o host para filtrar a lista de recursos e clique em **Atualizar recursos**.

Os sistemas de arquivos recém-adicionados, renomeados ou excluídos são atualizados para o inventário do SnapCenter Server.

Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

Crie políticas de backup para sistemas de arquivos do Windows

Você pode criar uma nova política de backup para recursos antes de usar o SnapCenter para fazer backup de sistemas de arquivos do Windows ou pode criar uma nova política de backup no momento em que cria um grupo de recursos ou quando faz backup de um recurso.

Antes de começar

- Você deve ter definido sua estratégia de backup."Saber mais"
- Você deve estar preparado para a proteção de dados.

  Para se preparar para a proteção de dados, você deve concluir tarefas como instalar o SnapCenter, adicionar hosts, descobrir recursos e criar conexões de máquina virtual de armazenamento (SVM).

- Se você estiver replicando Snapshots para um espelho ou armazenamento secundário de cofre, o administrador do SnapCenter deverá ter atribuído as SVMs a você para os volumes de origem e destino.
- Se você quiser executar os scripts do PowerShell em prescripts e postscripts, defina o valor do parâmetro usePowershellProcessforScripts como true no arquivo web.config.

  O valor padrão é falso

- Revise os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror . Para obter informações, consulte "Limites de objetos para sincronização ativa do SnapMirror" .

Sobre esta tarefa

- O SCRIPTS_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCoreServiceHost.exe.Config do host do plug-in.

  Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável que você use o caminho padrão por segurança.

  O valor da chave pode ser exibido no swagger por meio da API: API /4.7/configsettings

  Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

- SnapLock
  - Se a opção 'Manter as cópias de backup por um número específico de dias' for selecionada, o período de retenção do SnapLock deverá ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio de Snapshot impede a exclusão dos Snapshots até que o período de retenção expire. Isso pode levar à retenção de um número maior de Snapshots do que a contagem especificada na política.
  - Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, selecione **Configurações**.
2. Na página Configurações, selecione **Políticas**.
3. Selecione **Novo**.
4. Na página Nome, insira o nome e os detalhes da política.
5. Na página Backup e Replicação, execute as seguintes tarefas:

   a. Selecione uma configuração de backup.

Opção	Descrição
Backup consistente do sistema de arquivos	Escolha esta opção se desejar que o SnapCenter desative a unidade de disco na qual o sistema de arquivos reside antes do início da operação de backup e, em seguida, retome a unidade de disco após o término da operação de backup.
Backup consistente com falhas do sistema de arquivos	Escolha esta opção se não quiser que o SnapCenter desative a unidade de disco na qual o sistema de arquivos reside.

   b. Selecione uma frequência de programação (também chamada de tipo de política).

      A política especifica apenas a frequência de backup. O cronograma de proteção específico para backup é definido no grupo de recursos. Portanto, dois ou mais grupos de recursos podem compartilhar a mesma política e frequência de backup, mas ter agendamentos de backup diferentes.

      Se você agendou para 2h00, a programação não será acionada durante o horário de verão (DST).

   c. Selecione um rótulo de política.

      Dependendo do rótulo do Snapshot selecionado, o ONTAP aplica a política de retenção do Snapshot secundário que corresponde ao rótulo.

      Se você selecionou **Atualizar SnapMirror após criar uma cópia local do Snapshot**, você pode opcionalmente especificar o rótulo da política secundária. No entanto, se você tiver selecionado **Atualizar SnapVault após criar uma cópia local do Snapshot**, deverá especificar o rótulo da política secundária.

6. Na seção Selecionar opções de replicação secundária, selecione uma ou ambas as seguintes opções de replicação secundária:

Para este campo…	Faça isso…
Atualizar o SnapMirror após criar uma cópia local do Snapshot	Selecione esta opção para criar cópias espelhadas de conjuntos de backup em outro volume (SnapMirror). Esta opção deve ser habilitada para sincronização ativa do SnapSnapMirror. Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Ver "Veja backups e clones relacionados na página Topologia" .
Atualizar o SnapVault após criar uma cópia do Snapshot	Selecione esta opção para executar a replicação de backup de disco para disco. Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão Atualizar na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Quando o SnapLock é configurado somente no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão Atualizar na página Topologia atualiza o período de bloqueio no secundário recuperado do ONTAP. Para mais informações sobre o SnapLock Vault, consulte "Enviar cópias do Snapshot para o WORM em um destino de cofre"
Contagem de novas tentativas de erro	Insira o número de tentativas de replicação que devem ocorrer antes que o processo seja interrompido.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o armazenamento secundário para evitar atingir o limite máximo de Snapshots no armazenamento secundário.

7. Na página Configurações de retenção, especifique as configurações de retenção para backups sob demanda e para cada frequência de agendamento selecionada.

Opção	Descrição
Total de cópias do Snapshot a serem mantidas	Escolha esta opção se quiser especificar o número de Snapshots que o SnapCenter armazena antes de excluí-los automaticamente.
Mantenha cópias do Snapshot para	Escolha esta opção se quiser especificar o número de dias que o SnapCenter retém uma cópia de backup antes de excluí-la.
Período de bloqueio de cópia de instantâneo	Selecione Período de bloqueio do instantâneo e especifique a duração em dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

Você deve definir a contagem de retenção como 2 ou mais. O valor mínimo para a contagem de retenção é 2.

O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida como um valor maior do que o suportado pela versão do ONTAP .

8. Na página Script, insira o caminho do prescript ou postscript que você deseja que o SnapCenter Server execute antes ou depois da operação de backup, respectivamente, e um limite de tempo que o SnapCenter aguarda a execução do script antes de atingir o tempo limite.

   Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas e enviar logs.

   O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_PATH.

9. Revise o resumo e clique em **Concluir**.

Criar grupos de recursos para sistemas de arquivos do Windows

Um grupo de recursos é o contêiner ao qual você pode adicionar vários sistemas de arquivos que deseja proteger. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que deseja executar e, em seguida, especificar o agendamento de backup.

Sobre esta tarefa

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .
- Não há suporte para adicionar novos sistemas de arquivos sem sincronização ativa do SnapMirror a um grupo de recursos existente que contém recursos com sincronização ativa do SnapMirror .
- Não há suporte para adicionar novos sistemas de arquivos a um grupo de recursos existente no modo de failover da sincronização ativa do SnapMirror . Você pode adicionar recursos ao grupo de recursos somente no estado regular ou de failback.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Sistemas de arquivos** na lista.

   Se você adicionou recentemente um sistema de arquivos ao SnapCenter, clique em **Atualizar recursos** para visualizar o recurso recém-adicionado.

3. Clique em **Novo Grupo de Recursos**.
4. Na página Nome do assistente, faça o seguinte:

Para este campo…	Faça isso…
Nome	Digite o nome do grupo de recursos. O nome do grupo de recursos não deve exceder 250 caracteres.
Use formato de nome personalizado para cópia do Snapshot	Opcional: insira um nome e formato de Snapshot personalizado. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.
Marcação	Insira uma tag descritiva para ajudar a encontrar um grupo de recursos.

5. Na página Recursos, execute as seguintes tarefas:

   a. Selecione o host para filtrar a lista de recursos.

      Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

   b. Na seção Recursos disponíveis, clique nos sistemas de arquivos dos quais deseja fazer backup e, em seguida, clique na seta para a direita para movê-los para a seção Adicionados.

      Se você selecionar a opção **Selecionar automaticamente todos os recursos no mesmo volume de armazenamento**, todos os recursos no mesmo volume serão selecionados. Quando você os move para a seção Adicionados, todos os recursos naquele volume são movidos juntos.

   Para adicionar um único sistema de arquivos, desmarque a opção **Selecionar automaticamente todos os recursos no mesmo volume de armazenamento** e selecione os sistemas de arquivos que deseja mover para a seção Adicionados.

6. Na página Políticas, execute as seguintes tarefas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você pode selecionar qualquer política existente e clicar em **Detalhes** para determinar se pode usar

essa política.

Se nenhuma política existente atender às suas necessidades, você pode criar uma nova política clicando em * + * para iniciar o assistente de política.

As políticas selecionadas são listadas na coluna Política na seção Configurar agendamentos para políticas selecionadas.

b. Na seção Configurar agendamentos para políticas selecionadas, clique em * + * na coluna Configurar agendamentos da política para a qual você deseja configurar o agendamento.

c. Se a política estiver associada a vários tipos de agendamento (frequências), selecione a frequência que deseja configurar.

d. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento especificando a data de início, a data de expiração e a frequência e clique em **Concluir**.

Os agendamentos configurados são listados na coluna Agendamentos aplicados na seção Configurar agendamentos para políticas selecionadas.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter . Você não deve modificar os agendamentos do agendador de tarefas do Windows e do SQL Server Agent.

7. Na página Notificação, forneça informações de notificação, da seguinte forma:

Para este campo…	**Faça isso…**
Preferência de e-mail	Selecione **Sempre**, **Em caso de falha** ou **Em caso de falha ou aviso** para enviar e-mails aos destinatários após criar grupos de recursos de backup, anexar políticas e configurar agendamentos. Insira o servidor SMTP, a linha de assunto do e-mail padrão e os endereços de e-mail De e Para.
De	Endereço de email
Para	Endereço de e-mail
Assunto	Assunto padrão do e-mail

8. Revise o resumo e clique em **Concluir**.

Você pode executar um backup sob demanda ou aguardar a ocorrência do backup agendado.

Crie grupos de recursos e habilite a proteção secundária para sistemas de arquivos do Windows em sistemas ASA r2

Você deve criar o grupo de recursos para adicionar os recursos que estão nos sistemas ASA r2. Você também pode provisionar a proteção secundária ao criar o grupo de

recursos.

Antes de começar

- Você deve garantir que não está adicionando recursos do ONTAP 9.x e recursos do ASA r2 ao mesmo grupo de recursos.
- Você deve garantir que não tenha um banco de dados com recursos ONTAP 9.x e recursos ASA r2.

Sobre esta tarefa

- A proteção secundária estará disponível somente se o usuário conectado estiver atribuído à função que tem o recurso **SecondaryProtection** habilitado.
- Se você habilitar a proteção secundária, o grupo de recursos será colocado no modo de manutenção durante a criação dos grupos de consistência primário e secundário. Depois que os grupos de consistência primário e secundário são criados, o grupo de recursos é retirado do modo de manutenção.
- O SnapCenter não oferece suporte à proteção secundária para um recurso clone.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:
   a. Insira um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 caracteres.

   b. Insira um ou mais rótulos no campo Tag para ajudar você a pesquisar o grupo de recursos posteriormente.

      Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.

   c. Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

      Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

   d. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

      Você deve usar exatamente o mesmo destino definido no aplicativo, incluindo o prefixo, se necessário.

4. Na página Recursos, selecione o nome do host do banco de dados na lista suspensa **Host**.

   Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos do ASA r2 na seção Recursos disponíveis e mova-os para a seção Recursos selecionados.
6. Na página Configurações do aplicativo, selecione a opção de backup.

7. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em + .

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

   c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

      Onde *policy_name* é o nome da política que você selecionou.

      Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

   Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Se a proteção secundária estiver habilitada para a política selecionada, a página Proteção Secundária será exibida e você precisará executar as seguintes etapas:

   a. Selecione o tipo de política de replicação.

      A política de replicação síncrona não é suportada.

   b. Especifique o sufixo do grupo de consistência que você deseja usar.

   c. Nos menus suspensos Cluster de destino e SVM de destino, selecione o cluster emparelhado e o SVM que você deseja usar.

      O cluster e o peering de SVM não são suportados pelo SnapCenter. Você deve usar o System Manager ou as CLIs do ONTAP para executar o peering de cluster e SVM.

Se os recursos já estiverem protegidos fora do SnapCenter, eles serão exibidos na seção Recursos Protegidos Secundários.

1. Na página Verificação, execute as seguintes etapas:

   a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para realizar a verificação no armazenamento secundário.

   b. Clique + na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política.

   c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name, execute as seguintes ações:

Se você quiser…	Faça isso…
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

d. Selecione **Verificar no local secundário** para verificar seus backups no sistema de armazenamento secundário.

e. Clique em **OK**.

Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

2. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

3. Revise o resumo e clique em **Concluir**.

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell

Você deve criar uma conexão de máquina virtual de armazenamento (SVM) e uma credencial antes de usar cmdlets do PowerShell para executar operações de proteção de dados.

Antes de começar

- Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.
- Você deve ter as permissões necessárias na função de administrador de infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estejam em andamento.

  As instalações do plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento porque o cache do host pode não ser atualizado e o status dos bancos de dados pode ser exibido na GUI do SnapCenter como “Não disponível para backup” ou "`Não no armazenamento NetApp ".

- Os nomes dos sistemas de armazenamento devem ser exclusivos.

  O SnapCenter não oferece suporte a vários sistemas de armazenamento com o mesmo nome em clusters diferentes. Cada sistema de armazenamento suportado pelo SnapCenter deve ter um nome exclusivo e um endereço IP LIF de gerenciamento exclusivo.

Passos

1. Inicie uma sessão de conexão do PowerShell Core usando o cmdlet Open-SmConnection.

   Este exemplo abre uma sessão do PowerShell:

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

2. Crie uma nova conexão com o sistema de armazenamento usando o cmdlet Add-SmStorageConnection.

   Este exemplo cria uma nova conexão de sistema de armazenamento:

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Crie uma nova credencial usando o cmdlet Add-SmCredential.

   Este exemplo cria uma nova credencial chamada FinanceAdmin com credenciais do Windows:

   ```
   PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup de um único recurso sob demanda para sistemas de arquivos do Windows

Se um recurso não estiver em um grupo de recursos, você poderá fazer backup do recurso sob demanda na página Recursos.

Sobre esta tarefa

Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com armazenamento secundário, a função atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.

> Ao fazer backup de um sistema de arquivos, o SnapCenter não faz backup de LUNs que estão montados em um ponto de montagem de volume (VMP) no sistema de arquivos que está sendo feito backup.

> Se você estiver trabalhando em um contexto de sistema de arquivos do Windows, não faça backup dos arquivos de banco de dados. Isso cria um backup inconsistente e uma possível perda de dados durante a restauração. Para proteger arquivos de banco de dados, você deve usar o plug-in SnapCenter apropriado para o banco de dados (por exemplo, SnapCenter Plug-in para Microsoft SQL Server ou SnapCenter Plug-in para Microsoft Exchange Server).

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o tipo de recurso Sistema de arquivos e, em seguida, selecione o recurso do qual deseja fazer backup.
3. Se o assistente Sistema de Arquivos - Proteger não iniciar automaticamente, clique em **Proteger** para iniciar o assistente.

   Especifique as configurações de proteção, conforme descrito nas tarefas de criação de grupos de recursos.

4. Opcional: Na página Recurso do assistente, insira um formato de nome personalizado para o Snapshot.

   Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

5. Na página Políticas, execute as seguintes tarefas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você pode selecionar qualquer política existente e clicar em **Detalhes** para determinar se pode usar essa política.

      Se nenhuma política existente atender aos seus requisitos, você pode copiar uma política existente e modificá-la ou criar uma nova política clicando em + para iniciar o assistente de política. Se nenhuma política existente atender aos seus requisitos, você pode copiar uma política existente e modificá-la ou criar uma nova política clicando em + para iniciar o assistente de política.

      As políticas selecionadas são listadas na coluna Política na seção Configurar agendamentos para políticas selecionadas.

   b. Na seção Configurar agendamentos para políticas selecionadas, clique em + na coluna Configurar agendamentos da política para a qual você deseja configurar o agendamento.

   c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento especificando a data de início, a data de expiração e a frequência e clique em **Concluir**.

      Os agendamentos configurados são listados na coluna Agendamentos aplicados na seção Configurar agendamentos para políticas selecionadas.

   "As operações programadas podem falhar"

6. Na página Notificação, execute as seguintes tarefas:

Para este campo…	Faça isso…
Preferência de e-mail	Selecione **Sempre**, ou **Em caso de falha**, ou **Em caso de falha ou aviso**, para enviar e-mails aos destinatários após criar grupos de recursos de backup, anexar políticas e configurar agendamentos. Insira as informações do servidor SMTP, a linha de assunto do e-mail padrão e os endereços de e-mail "Para" e "De".
De	Endereço de email
Para	Endereço de e-mail
Assunto	Assunto padrão do e-mail

7. Revise o resumo e clique em **Concluir**.

   A página de topologia do banco de dados é exibida.

8. Clique em **Fazer backup agora**.
9. Na página Backup, execute as seguintes etapas:
   a. Se você aplicou várias políticas ao recurso, na lista suspensa Política, selecione a política que deseja usar para backup.

      Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

   b. Clique em **Backup**.
10. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

   O prompt de nome de usuário e senha é exibido.

2. Crie uma política de backup usando o cmdlet Add-SmPolicy.

   Este exemplo cria uma nova política de backup com um tipo de backup SQL de FullBackup:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

Este exemplo cria uma nova política de backup com um tipo de backup do sistema de arquivos do Windows de CrashConsistent:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Descubra recursos do host usando o cmdlet Get-SmResources.

   Este exemplo descobre os recursos para o plug-in Microsoft SQL no host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

   Este exemplo descobre os recursos para sistemas de arquivos do Windows no host especificado:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Adicione um novo grupo de recursos ao SnapCenter usando o cmdlet Add-SmResourceGroup.

   Este exemplo cria um novo grupo de recursos de backup de banco de dados SQL com a política e os recursos especificados:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

   Este exemplo cria um novo grupo de recursos de backup do sistema de arquivos do Windows com a política e os recursos especificados:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Inicie uma nova tarefa de backup usando o cmdlet New-SmBackup.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Visualize o status do trabalho de backup usando o cmdlet Get-SmBackupReport.

   Este exemplo exibe um relatório de resumo de todos os trabalhos que foram executados na data especificada:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup de grupos de recursos para sistemas de arquivos do Windows

Um grupo de recursos é uma coleção de recursos em um host ou cluster. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos. Você pode fazer backup de um grupo de recursos sob demanda na página Recursos. Se um grupo de recursos tiver uma política anexada e um agendamento configurado, os backups ocorrerão automaticamente de acordo com o agendamento.

Antes de começar

- Você deve ter criado um grupo de recursos com uma política anexada.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com o armazenamento secundário, a função atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.
- Se um grupo de recursos tiver vários bancos de dados de hosts diferentes, a operação de backup em alguns dos hosts poderá ser acionada tardiamente devido a problemas de rede. Você deve configurar o valor de MaxRetryForUninitializedHosts em web.config usando o cmdlet Set-SmConfigSettings do PowerShell

Ao fazer backup de um sistema de arquivos, o SnapCenter não faz backup de LUNs que estão montados em um ponto de montagem de volume (VMP) no sistema de arquivos que está sendo feito backup.

Se você estiver trabalhando em um contexto de sistema de arquivos do Windows, não faça backup dos arquivos de banco de dados. Isso cria um backup inconsistente e uma possível perda de dados durante a restauração. Para proteger arquivos de banco de dados, você deve usar o plug-in SnapCenter apropriado para o banco de dados (por exemplo, SnapCenter Plug-in para Microsoft SQL Server ou SnapCenter Plug-in para Microsoft Exchange Server).

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.

   Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou clicando em e selecionando a tag. Você pode então clicar para fechar o painel de filtro.

3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e clique em **Fazer backup agora**.

   Para o SnapCenter Plug-in para Oracle Database, se você tiver um grupo de recursos federados com dois bancos de dados e um deles tiver um arquivo de dados em um armazenamento não NetApp , a operação de backup será abortada mesmo que o outro banco de dados esteja em um armazenamento NetApp .

4. Na página Backup, execute as seguintes etapas:
   a. Se você tiver associado várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

      Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

   b. Clique em **Backup**.
5. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.
   - Nas configurações do MetroCluster , o SnapCenter pode não conseguir detectar um relacionamento de proteção após um failover.

     "Não é possível detectar o relacionamento SnapMirror ou SnapVault após failover do MetroCluster"

   - Se você estiver fazendo backup de dados do aplicativo em VMDKs e o tamanho do heap Java para o SnapCenter Plug-in for VMware vSphere não for grande o suficiente, o backup poderá falhar. Para aumentar o tamanho do heap Java, localize o arquivo de script `/opt/netapp/init_scripts/scvservice` . Nesse roteiro, o `do_start method` O comando inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: `Java -jar -Xmx8192M -Xms4096M` .

Monitorar operações de backup

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Talvez você queira verificar o progresso para determinar quando ele foi concluído ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado correspondente das operações:

- Em andamento
- Concluído com sucesso
- Fracassado
-

Concluído com avisos ou não pôde ser iniciado devido a avisos

- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **Trabalhos**.
3. Na página Trabalhos, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de backup sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Backup**.
   d. No menu suspenso **Status**, selecione o status do backup.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione uma tarefa de backup e clique em **Detalhes** para visualizar os detalhes da tarefa.

   Embora o status do trabalho de backup seja exibido , ao clicar em detalhes do trabalho, você poderá ver que algumas das tarefas filhas da operação de backup ainda estão em andamento ou marcadas com sinais de alerta.

5. Na página Detalhes do trabalho, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Monitorar operações no painel Atividade

O painel Atividade exibe as cinco operações mais recentes realizadas. O painel Atividade também exibe quando a operação foi iniciada e o status da operação.

O painel Atividade exibe informações sobre operações de backup, restauração, clonagem e backup agendado.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Clique no painel Atividade para visualizar as cinco operações mais recentes.

   Quando você clica em uma das operações, os detalhes da operação são listados na página **Detalhes do trabalho**.

Cancelar operações de backup

Você pode cancelar operações de backup que estão na fila.

O que você vai precisar

- Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar operações.

- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de backup em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** fica desabilitado para operações que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de backup enfileiradas de outros membros enquanto estiver usando essa função.

Passos

1. Execute uma das seguintes ações:

Do…	Ação
Página do monitor	a. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. b. Selecione a operação e clique em **Cancelar trabalho**.
Painel de atividades	a. Após iniciar a operação de backup, clique em *  * no painel Atividade para visualizar as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

A operação é cancelada e o recurso é revertido ao estado anterior.

Veja backups e clones relacionados na página Topologia

Ao se preparar para fazer backup ou clonar um recurso, você pode visualizar uma representação gráfica de todos os backups e clones no armazenamento primário e secundário. Na página Topologia, você pode ver todos os backups e clones disponíveis para o recurso ou grupo de recursos selecionado. Você pode visualizar os detalhes desses backups e clones e selecioná-los para executar operações de proteção de dados.

Sobre esta tarefa

Você pode revisar os seguintes ícones na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no armazenamento primário ou secundário (cópias espelhadas ou cópias do Vault).

-  exibe o número de backups e clones que estão disponíveis no armazenamento primário.
-

 exibe o número de backups e clones que são espelhados no armazenamento secundário usando a tecnologia SnapMirror .

> Clones de um backup de um espelho flexível em termos de versão em um volume do tipo mirror-vault são exibidos na exibição de topologia, mas a contagem de backups de espelho na exibição de topologia não inclui o backup flexível em termos de versão.

-  exibe o número de backups e clones que são replicados no armazenamento secundário usando a tecnologia SnapVault .
  - O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou 6 backups usando uma política para manter apenas 4 backups, o número de backups exibidos será 6.

> Clones de um backup de um espelho flexível em termos de versão em um volume do tipo mirror-vault são exibidos na exibição de topologia, mas a contagem de backups de espelho na exibição de topologia não inclui o backup flexível em termos de versão.

Se você tiver um relacionamento secundário como sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC]), poderá ver os seguintes ícones adicionais:

-  O site de réplica está no ar.
-  O site de réplicas está fora do ar.
-  O espelho secundário ou o relacionamento do cofre não foram restabelecidos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso na exibição de detalhes do recurso ou na exibição de detalhes do grupo de recursos.

   Se o recurso estiver protegido, a página de topologia do recurso selecionado será exibida.

4. Revise o cartão Resumo para ver um resumo do número de backups e clones disponíveis no armazenamento primário e secundário.

   A seção Cartão de Resumo exibe o número total de backups e clones. Somente para o banco de dados Oracle, a seção Cartão de Resumo também exibe o número total de backups de log.

   Clicar no botão **Atualizar** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clicar no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Uma programação semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo estiver distribuído em vários volumes, o tempo de expiração do SnapLock

para o backup será o maior tempo de expiração do SnapLock definido para um Snapshot em um volume. O maior tempo de expiração do SnapLock é recuperado do ONTAP.

Para sincronização ativa do SnapMirror , clicar no botão **Atualizar** atualiza o inventário de backup do SnapCenter consultando o ONTAP para sites primários e de réplica. Uma programação semanal também executa essa atividade para todos os bancos de dados que contêm o relacionamento de sincronização ativo do SnapMirror .

- Para sincronização ativa do SnapMirror e somente para o ONTAP 9.14.1, os relacionamentos Async Mirror ou Async MirrorVault com o novo destino primário devem ser configurados manualmente após o failover. A partir do ONTAP 9.15.1, o Async Mirror ou o Async MirrorVault são configurados automaticamente para o novo destino principal.
- Após o failover, um backup deve ser criado para que o SnapCenter esteja ciente do failover. Você pode clicar em **Atualizar** somente após um backup ter sido criado.

5. Na exibição Gerenciar cópias, clique em **Backups** ou **Clones** do armazenamento primário ou secundário para ver detalhes de um backup ou clone.

   Os detalhes dos backups e clones são exibidos em formato de tabela.

6. Selecione o backup na tabela e clique nos ícones de proteção de dados para executar operações de restauração, clonagem, renomeação e exclusão.

   Não é possível renomear ou excluir backups que estejam no sistema de armazenamento secundário.

7. Se você quiser excluir um clone, selecione o clone da tabela e clique em para excluir o clone.

Exemplo mostrando backups e clones no armazenamento primário

Limpe a contagem de backups secundários usando cmdlets do PowerShell

Você pode usar o cmdlet Remove-SmBackup para limpar a contagem de backups para backups secundários que não têm Snapshot. Talvez você queira usar este cmdlet quando o total de Snapshots exibidos na topologia Gerenciar Cópias não corresponder à configuração de retenção de Snapshot do armazenamento secundário.

Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Limpe a contagem de backups secundários usando o parâmetro -CleanupSecondaryBackups.

   Este exemplo limpa a contagem de backups para backups secundários sem instantâneos:

```
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"):
```

Restaurar sistemas de arquivos do Windows

Restaurar backups do sistema de arquivos do Windows

Você pode usar o SnapCenter para restaurar backups do sistema de arquivos. A restauração do sistema de arquivos é um processo multifásico que copia todos os dados de um backup especificado para o local original do sistema de arquivos.

Antes de começar

- Você deve ter feito backup do sistema de arquivos.
- Se uma operação agendada, como uma operação de backup, estiver em andamento para um sistema de arquivos, essa operação deverá ser cancelada antes que você possa iniciar uma operação de restauração.
- Você só pode restaurar um backup do sistema de arquivos para o local original, não para um caminho alternativo.

  Não é possível restaurar um único arquivo de um backup porque o sistema de arquivos restaurado substitui todos os dados no local original do sistema de arquivos. Para restaurar um único arquivo de um backup do sistema de arquivos, você deve clonar o backup e acessar o arquivo no clone.

- Não é possível restaurar um sistema ou volume de inicialização.
- O SnapCenter pode restaurar sistemas de arquivos em um cluster do Windows sem deixar o grupo de cluster offline.

Sobre esta tarefa

- O SCRIPTS_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCoreServiceHost.exe.Config do host do plug-in.

  Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável que você use o caminho padrão por segurança.

O valor da chave pode ser exibido no swagger por meio da API: API /4.7/configsettings

Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

- Para a operação de restauração de sincronização ativa do SnapMirror , você deve selecionar o backup do local principal.
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Para filtrar a lista de recursos, selecione as opções Sistema de arquivos e Grupo de recursos.
3. Selecione um grupo de recursos na lista e clique em **Restaurar**.
4. Na página Backups, selecione se deseja restaurar dos sistemas de armazenamento primário ou secundário e, em seguida, selecione um backup para restaurar.
5. Selecione suas opções no assistente de restauração.
6. Você pode inserir o caminho e os argumentos do prescript ou postscript que deseja que o SnapCenter execute antes ou depois da operação de restauração, respectivamente.

   Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.

   O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_PATH.

7. Na página Notificação, selecione uma das seguintes opções:

Para este campo…	Faça isso…
Registrar eventos do servidor SnapCenter no syslog do sistema de armazenamento	Selecione esta opção para registrar eventos do SnapCenter Server no syslog do sistema de armazenamento.
Enviar notificação de AutoSupport para operações com falha no sistema de armazenamento	Selecione esta opção para enviar informações sobre quaisquer operações com falha para a NetApp usando o AutoSupport.
Preferência de e-mail	Selecione **Sempre**, **Em caso de falha** ou **Em caso de falha ou aviso** para enviar mensagens de e-mail aos destinatários após restaurar os backups. Insira o servidor SMTP, a linha de assunto do e-mail padrão e os endereços de e-mail De e Para.

8. Revise o resumo e clique em **Concluir**.
9. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Se o sistema de arquivos restaurado contiver um banco de dados, você também deverá restaurar o banco de dados. Se você não restaurar o banco de dados, ele poderá estar em um estado inválido. Para obter informações sobre como restaurar bancos de dados, consulte o Guia de Proteção de Dados desse banco de dados.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o

cmdlet Open-SmConnection.

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

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
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
```

   Este exemplo exibe informações detalhadas sobre o backup de 29 de janeiro de 2015 a 3 de fevereiro de 2015:

```
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. Restaure os dados do backup usando o cmdlet Restore-SmBackup.

```
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          :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Restaurar recursos usando cmdlets do PowerShell

Restaurar um backup de recursos inclui iniciar uma sessão de conexão com o SnapCenter Server, listar os backups e recuperar informações de backup, além de restaurar um backup.

Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
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
```

   Este exemplo exibe informações detalhadas sobre o backup de 29 de janeiro de 2015 a 3 de fevereiro de 2015:

```
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. Restaure os dados do backup usando o cmdlet Restore-SmBackup.

```
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          :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitorar operações de restauração

Você pode monitorar o progresso de diferentes operações de restauração do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa tomar.

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento

- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de restauração sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Restaurar**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Aplicar** para visualizar as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Cancelar operações de restauração

Você pode cancelar trabalhos de restauração que estão na fila.

Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações de restauração.

Sobre esta tarefa

- Você pode cancelar uma operação de restauração enfileirada na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de restauração em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de restauração enfileiradas.
- O botão **Cancelar tarefa** fica desabilitado para operações de restauração que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de restauração enfileiradas de outros membros enquanto estiver usando essa função.

Etapa

Execute uma das seguintes ações:

Do…	Ação
Página do monitor	1. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. 2. Selecione o trabalho e clique em **Cancelar trabalho**.
Painel de atividades	1. Após iniciar a operação de restauração, clique em no painel Atividade para visualizar as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

Clonar sistemas de arquivos do Windows

Clonar a partir de um backup do sistema de arquivos do Windows

Você pode usar o SnapCenter para clonar um backup do sistema de arquivos do Windows. Se você quiser uma cópia de um único arquivo que foi excluído ou alterado por engano, você pode clonar um backup e acessar esse arquivo no clone.

Antes de começar

- Você deve ter se preparado para a proteção de dados concluindo tarefas como adicionar hosts, identificar recursos e criar conexões de máquina virtual de armazenamento (SVM).
- Você deve ter um backup do sistema de arquivos.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de armazenamento (SVM).
- Não é possível clonar um grupo de recursos. Você só pode clonar backups individuais do sistema de arquivos.
- Se um backup residir em uma máquina virtual com um disco VMDK, o SnapCenter não poderá clonar o backup em um servidor físico.
- Se você clonar um cluster do Windows (por exemplo, um LUN compartilhado ou um LUN de volume compartilhado de cluster (CSV)), o clone será armazenado como um LUN dedicado no host especificado.
- Para uma operação de clonagem, o diretório raiz do ponto de montagem do volume não pode ser um diretório compartilhado.
- Não é possível criar um clone em um nó que não seja o nó inicial do agregado.
- Não é possível agendar operações recorrentes de clonagem (ciclo de vida do clone) para sistemas de arquivos do Windows; você só pode clonar um backup sob demanda.
- Se você mover um LUN que contém um clone para um novo volume, o SnapCenter não poderá mais suportar o clone. Por exemplo, você não pode usar o SnapCenter para excluir esse clone.
- Não é possível clonar entre ambientes. Por exemplo, clonagem de um disco físico para um disco virtual ou vice-versa.

Sobre esta tarefa

- O SCRIPTS_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCoreServiceHost.exe.Config do host do plug-in.

  Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável que você use o caminho padrão por segurança.

  O valor da chave pode ser exibido no swagger por meio da API: API /4.7/configsettings

  Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Sistemas de arquivos** na lista.
3. Selecione o host.

   A visualização da topologia é exibida automaticamente se o recurso estiver protegido.

4. Na lista de recursos, selecione o backup que você deseja clonar e clique no ícone de clonagem.
5. Na página Opções, faça o seguinte:

Para este campo…	Faça isso…
Servidor clone	Escolha o host no qual o clone deve ser criado.
“Atribuir automaticamente ponto de montagem” ou “Atribuir automaticamente ponto de montagem de volume no caminho”	Escolha se deseja atribuir automaticamente um ponto de montagem ou um ponto de montagem de volume em um caminho. Atribuição automática de ponto de montagem de volume no caminho: O ponto de montagem em um caminho permite que você forneça um diretório específico no qual os pontos de montagem serão criados. Antes de escolher esta opção, você deve verificar se o diretório está vazio. Se houver um backup no diretório, o backup ficará em um estado inválido após a operação de montagem.
Localização do arquivo	Escolha um local de arquivamento se estiver clonando um backup secundário.

6. Na página Script, especifique quaisquer prescrições ou pós-escritos que você deseja executar.

   O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_PATH.

7. Revise o resumo e clique em **Concluir**.
8. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Liste os backups que podem ser clonados usando o cmdlet Get-SmBackup ou Get-SmResourceGroup.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                      BackupTime   BackupType
--------   ----------                      ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

   Este exemplo exibe informações sobre um grupo de recursos especificado, seus recursos e políticas associadas:

```
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. Inicie uma operação de clonagem de um backup existente usando o cmdlet New-SmClone.

   Este exemplo cria um clone de um backup especificado com todos os logs:

```
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
```

   Este exemplo cria um clone para uma instância especificada do Microsoft SQL Server:

```
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. Visualize o status do trabalho de clonagem usando o cmdlet Get-SmCloneReport.

   Este exemplo exibe um relatório de clone para o ID do trabalho especificado:

```
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}
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitorar operações de clonagem

Você pode monitorar o progresso das operações de clonagem do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente operações de clonagem sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione o trabalho de clonagem e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página Detalhes do trabalho, clique em **Exibir registros**.

Cancelar operações de clonagem

Você pode cancelar operações de clonagem que estão na fila.

Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar operações de clonagem.

Sobre esta tarefa

- Você pode cancelar uma operação de clone enfileirada na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de clonagem em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de clonagem enfileiradas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de clonagem enfileiradas de outros membros enquanto estiver usando essa função.

Etapa

Execute uma das seguintes ações:

Do…	Ação
Página do monitor	1. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. 2. Selecione a operação e clique em **Cancelar trabalho**.

Do…	Ação
Painel de atividades	1. Após iniciar a operação de clonagem, clique em no painel Atividade para visualizar as cinco operações mais recentes. 2. Selecione a operação. 3. Na página **Detalhes do trabalho**, clique em **Cancelar trabalho**.

Dividir um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido se torna independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clone em um clone intermediário.

  Por exemplo, depois de criar o clone1 a partir de um backup de banco de dados, você pode criar um backup do clone1 e então clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e você não pode executar a operação de divisão de clone no clone1. No entanto, você pode executar a operação de divisão de clone no clone2.

  Após dividir o clone2, você pode executar a operação de divisão do clone no clone1 porque o clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e os trabalhos de clonagem do clone são excluídos.
- Para obter informações sobre as operações de divisão de volume do FlexClone , consulte "Dividir um volume FlexClone de seu volume pai" .
- Certifique-se de que o volume ou agregado no sistema de armazenamento esteja online.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página **Recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicações de banco de dados	Selecione **Banco de dados** na lista Exibir.
Para sistemas de arquivos	Selecione **Caminho** na lista Exibir.

3. Selecione o recurso apropriado na lista.

   A página de topologia de recursos é exibida.

4. Na exibição **Gerenciar cópias**, selecione o recurso clonado (por exemplo, o banco de dados ou LUN) e clique em * *.
5. Revise o tamanho estimado do clone que será dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.

6. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

   A operação de divisão do clone para de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clone e, em seguida, tentar novamente a operação de divisão de clone.

   Se você quiser um tempo de pesquisa maior ou menor para verificar se o clone está dividido ou não, você pode alterar o valor do parâmetro *CloneSplitStatusCheckPollTime* no arquivo *SMCoreServiceHost.exe.config* para definir o intervalo de tempo para o SMCore pesquisar o status da operação de divisão do clone. O valor está em milissegundos e o valor padrão é 5 minutos.

   Por exemplo:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   A operação de início da divisão do clone falha se um backup, uma restauração ou outra divisão do clone estiver em andamento. Você deve reiniciar a operação de divisão do clone somente após a conclusão das operações em execução.

Informações relacionadas

"O clone ou a verificação do SnapCenter falham com o agregado inexistente"

Proteja os bancos de dados do Microsoft Exchange Server

Conceitos do plug-in SnapCenter para Microsoft Exchange Server

Visão geral do plug-in SnapCenter para Microsoft Exchange Server

O SnapCenter Plug-in para Microsoft Exchange Server é um componente do lado do host do NetApp SnapCenter Software que permite o gerenciamento de proteção de dados com reconhecimento de aplicativo de bancos de dados do Exchange. O Plug-in para Exchange automatiza o backup e a restauração de bancos de dados do Exchange no seu ambiente SnapCenter .

Quando o Plug-in para Exchange estiver instalado, você poderá usar o SnapCenter com a tecnologia NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia NetApp SnapVault para executar a replicação de backup de disco para disco para fins de conformidade com padrões ou arquivamento.

Se você quiser restaurar e recuperar e-mails ou caixas de correio em vez do banco de dados completo do Exchange, poderá usar o software Single Mailbox Recovery (SMBR). O NetApp® Single Mailbox Recovery chegou ao fim da disponibilidade (EOA) em 12 de maio de 2023. A NetApp continuará a oferecer suporte aos clientes que adquiriram capacidade de caixa de correio, manutenção e suporte por meio de números de peça de marketing introduzidos em 24 de junho de 2020, durante a vigência do direito ao suporte.

O NetApp Single Mailbox Recovery é um produto parceiro fornecido pela Ontrack. O Ontrack PowerControls oferece recursos semelhantes aos do NetApp Single Mailbox Recovery. Os clientes podem adquirir novas licenças de software Ontrack PowerControls e renovações de manutenção e suporte do Ontrack PowerControls da Ontrack (por meio de licensingteam@ontrack.com) para recuperação granular de caixa de correio.

O plug-in para Exchange oferece suporte à sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC]), que permite que os serviços empresariais continuem operando mesmo durante uma falha completa do site, permitindo que os aplicativos façam failover de forma transparente usando uma cópia secundária. Não é necessária intervenção manual nem script adicional para acionar um failover com a sincronização ativa do SnapMirror .

Ele suporta o modo assimétrico, failover ou não duplex do SnapMirror Active Sync. Isso se refere à solução em que o caminho otimizado vem somente do nó proprietário do LUN do lado primário. Qualquer E/S proveniente dos caminhos do cluster secundário é atendida por proxy para o cluster primário. A replicação síncrona é unidirecional, na direção do primário para o secundário.

- Automatiza operações de backup e restauração com reconhecimento de aplicativo para bancos de dados do Microsoft Exchange Server e Grupos de Disponibilidade de Banco de Dados (DAGs) em seu ambiente SnapCenter
- Oferece suporte a servidores Exchange virtualizados em LUNs RDM quando você implanta o SnapCenter Plug-in for VMware vSphere e registra o plug-in com o SnapCenter.

O que você pode fazer com o plug-in SnapCenter para Microsoft Exchange Server

Você pode usar o Plug-in para Exchange para fazer backup e restaurar bancos de dados do Exchange Server.

- Visualize e gerencie um inventário ativo de Grupos de Disponibilidade de Banco de Dados (DAGs) do Exchange, bancos de dados e conjuntos de réplicas
- Defina políticas que forneçam as configurações de proteção para automação de backup
- Atribuir políticas a grupos de recursos
- Proteja DAGs e bancos de dados individuais
- Fazer backup de bancos de dados de caixa de correio primários e secundários do Exchange
- Restaurar bancos de dados de backups primários e secundários

Tipos de armazenamento suportados pelo SnapCenter Plug-in para Microsoft Windows e para Microsoft Exchange Server

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e virtuais. Você deve verificar se o suporte está disponível para seu tipo de armazenamento antes de instalar o pacote para seu host.

O suporte ao provisionamento e à proteção de dados do SnapCenter está disponível no Windows Server. Para obter as informações mais recentes sobre as versões suportadas, consulte o https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT [Ferramenta de Matriz de Interoperabilidade NetApp ^].

Máquina	Tipo de armazenamento	Provisão usando	Notas de suporte
Servidor físico	LUNs conectados por FC	Interface gráfica do usuário (GUI) do SnapCenter ou cmdlets do PowerShell	
Servidor físico	LUNs conectados por iSCSI	Cmdlets do SnapCenter GUI ou PowerShell	
VMware VM	LUNs RDM conectados por um FC ou iSCSI HBA	Cmdlets do PowerShell	Somente compatibilidade física VMDKs não são suportados.
VMware VM	LUNs iSCSI conectados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets do SnapCenter GUI ou PowerShell	VMDKs não são suportados.

Máquina	Tipo de armazenamento	Provisão usando	Notas de suporte
VM Hyper-V	LUNs FC virtuais (vFC) conectados por um switch Fibre Channel virtual	Cmdlets do SnapCenter GUI ou PowerShell	Você deve usar o Hyper-V Manager para provisionar LUNs de FC Virtual (vFC) conectados por um Switch de Canal de Fibra virtual. Não há suporte para discos de passagem do Hyper-V e backup de bancos de dados em VHD(x) provisionados no armazenamento NetApp .
VM Hyper-V	LUNs iSCSI conectados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets do SnapCenter GUI ou PowerShell	Não há suporte para discos de passagem do Hyper-V e backup de bancos de dados em VHD(x) provisionados no armazenamento NetApp .

Privilégios ONTAP mínimos necessários para o plug-in do Exchange

Os privilégios mínimos do ONTAP necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos de acesso total: privilégios mínimos necessários para ONTAP 9.12.1 e posterior
  - evento generate-autosupport-log
  - histórico de trabalho mostrar
  - parada de trabalho

- lua
- lun criar
- lun criar
- lun criar
- lun delete
- lun igroup adicionar
- lun igroup criar
- lun igroup excluir
- renomear lun igroup
- renomear lun igroup
- show do lun igroup
- mapeamento lun add-reporting-nodes
- criação de mapeamento lun
- exclusão de mapeamento lun
- mapeamento lun remove-reporting-nodes
- show de mapeamento lunar
- lun modificar
- volume de entrada lun
- lua offline
- lua online
- lun persistente-reserva clara
- redimensionamento de lun
- série lun
- show de lua
- política de adição de regra do snapmirror
- regra de modificação de política do snapmirror
- política de remoção do snapmirror
- política do snapmirror mostrar
- restauração do snapmirror
- show de espelhos instantâneos
- histórico de exibição do snapmirror
- atualização do snapmirror
- atualização do snapmirror-ls-set
- lista-destinos do snapmirror
- versão
- criação de clone de volume
- show de clones de volume

- volume clone split start
- volume clone divisão parada
- volume criar
- destruição de volume
- clone de arquivo de volume criar
- arquivo de volume mostrar-uso-do-disco
- volume offline
- volume on-line
- modificação de volume
- volume qtree criar
- volume qtree delete
- volume qtree modificar
- volume qtree mostrar
- restrição de volume
- show de volume
- criação de instantâneo de volume
- exclusão de instantâneo de volume
- modificação de instantâneo de volume
- instantâneo de volume modificar-tempo-de-expiração-do-snaplock
- renomeação de instantâneo de volume
- restauração de instantâneo de volume
- arquivo de restauração de instantâneo de volume
- exibição de instantâneo de volume
- desmontagem de volume
- cifs do vserver
- vserver cifs compartilhar criar
- vserver cifs compartilhar excluir
- vserver cifs shadowcopy mostrar
- vserver cifs compartilhar mostrar
- vserver cifs mostrar
- política de exportação do vserver
- criação de política de exportação do vserver
- exclusão da política de exportação do vserver
- criação de regra de política de exportação do vserver
- mostrar regra de política de exportação do vserver
- mostrar política de exportação do vserver
- vserver iscsi

- mostrar conexão iscsi do vserver
- vserver mostrar

- Comandos somente leitura: privilégios mínimos necessários para ONTAP 8.3.0 e posterior
  - interface de rede
  - exibição de interface de rede
  - vserver

Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault

Você pode usar um plug-in SnapCenter com a tecnologia ONTAP SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia ONTAP SnapVault para executar replicação de backup de disco para disco para conformidade com padrões e outros propósitos relacionados à governança. Antes de executar essas tarefas, você deve configurar um relacionamento de proteção de dados entre os volumes de origem e destino e inicializar o relacionamento.

O SnapCenter executa as atualizações no SnapMirror e no SnapVault após concluir a operação Snapshot. As atualizações do SnapMirror e do SnapVault são executadas como parte do trabalho do SnapCenter ; não crie uma programação ONTAP separada.

Se você estiver acessando o SnapCenter a partir de um produto NetApp SnapManager e estiver satisfeito com os relacionamentos de proteção de dados configurados, pode pular esta seção.

Um relacionamento de proteção de dados replica dados do armazenamento primário (o volume de origem) para o armazenamento secundário (o volume de destino). Quando você inicializa o relacionamento, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não oferece suporte a relacionamentos em cascata entre volumes SnapMirror e SnapVault (**Primário** > **Espelho** > **Cofre**). Você deve usar relacionamentos fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis em termos de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis em termos de versão e como configurá-los, consulte "Documentação do ONTAP" .

Definir uma estratégia de backup para recursos do Exchange Server

Definir uma estratégia de backup antes de criar suas tarefas de backup ajuda a garantir que você tenha os backups necessários para restaurar seus bancos de dados com sucesso. Seu Contrato de Nível de Serviço (SLA), Objetivo de Tempo de Recuperação (RTO) e Objetivo de Ponto de Recuperação (RPO) determinam em grande parte sua estratégia de backup.

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. O RTO é o momento em que um processo de negócios deve ser restaurado após uma interrupção no serviço. Um RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. O SLA, o RTO e o RPO contribuem para a estratégia de backup.

Tipos de backups suportados para banco de dados do Exchange

Para fazer backup de caixas de correio do Exchange usando o SnapCenter , é necessário escolher o tipo de recurso, como bancos de dados e Grupos de Disponibilidade de Banco de Dados (DAG). A tecnologia de instantâneo é utilizada para criar cópias on-line, somente leitura, dos volumes nos quais os recursos residem.

Tipo de backup	Descrição
Backup completo e de log	Faz backup dos bancos de dados e de todos os logs de transações, incluindo os logs truncados. Após a conclusão de um backup completo, o Exchange Server trunca os logs de transações que já estão confirmados no banco de dados. Normalmente, você deve escolher esta opção. No entanto, se o tempo de backup for curto, você pode optar por não executar um backup de log de transações com backup completo.
Backup completo	Faz backup de bancos de dados e logs de transações. Os logs de transações truncados não são copiados.
Backup de log	Faz backup de todos os logs de transações. Os logs truncados que já estão confirmados no banco de dados não são copiados. Se você agendar backups frequentes do log de transações entre backups completos do banco de dados, poderá escolher pontos de recuperação granulares.

Agendamentos de backup para plug-ins de banco de dados

A frequência de backup (tipo de agendamento) é especificada nas políticas; um agendamento de backup é especificado na configuração do grupo de recursos. O fator mais crítico na determinação da frequência ou programação de backup é a taxa de alteração do recurso e a importância dos dados. Você pode fazer backup de um recurso muito utilizado a cada hora, enquanto pode fazer backup de um recurso raramente utilizado uma vez por dia. Outros fatores incluem a importância do recurso para sua organização, seu Acordo de Nível de Serviço (SLA) e seu Objetivo de Ponto de Recuperação (RPO).

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. Um RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. O SLA e o RPO contribuem para a estratégia de proteção de dados.

Mesmo para um recurso muito utilizado, não há necessidade de executar um backup completo mais de uma ou duas vezes por dia. Por exemplo, backups regulares do log de transações podem ser suficientes para garantir que você tenha os backups necessários. Quanto mais você fizer backup dos seus bancos de dados, menos logs de transações o SnapCenter terá que usar no momento da restauração, o que pode resultar em operações de restauração mais rápidas.

Os agendamentos de backup têm duas partes, conforme a seguir:

- Frequência de backup

  A frequência de backup (com que frequência os backups devem ser realizados), chamada de *tipo de agendamento* para alguns plug-ins, faz parte de uma configuração de política. Você pode selecionar por hora, dia, semana ou mês como a frequência de backup da política. Se você não selecionar nenhuma dessas frequências, a política criada será somente sob demanda. Você pode acessar as políticas clicando em **Configurações** > **Políticas**.

- Agendamentos de backup

  Os agendamentos de backup (exatamente quando os backups devem ser executados) fazem parte de uma configuração de grupo de recursos. Por exemplo, se você tiver um grupo de recursos com uma política configurada para backups semanais, poderá configurar o agendamento para fazer backup toda quinta-feira às 22h. Você pode acessar as programações dos grupos de recursos clicando em **Recursos** > **Grupos de Recursos**.

Número de trabalhos de backup necessários para bancos de dados

Os fatores que determinam o número de tarefas de backup necessárias incluem o tamanho do recurso, o número de volumes usados, a taxa de alteração do recurso e seu Contrato de Nível de Serviço (SLA).

Convenções de nomenclatura de backup

Você pode usar a convenção de nomenclatura padrão do Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um registro de data e hora aos nomes de instantâneos que ajuda a identificar quando as cópias foram criadas.

O Snapshot usa a seguinte convenção de nomenclatura padrão:

```
resourcegroupname_hostname_timestamp
```

Você deve nomear seus grupos de recursos de backup logicamente, como no exemplo a seguir:

```
dts1_mach1x88_03-12-2015_23.17.26
```

Neste exemplo, os elementos de sintaxe têm os seguintes significados:

- *dts1* é o nome do grupo de recursos.
- *mach1x88* é o nome do host.
- *03-12-2015_23.17.26* é a data e o registro de data e hora.

Como alternativa, você pode especificar o formato do nome do Snapshot ao proteger recursos ou grupos de recursos selecionando **Usar formato de nome personalizado para cópia do Snapshot**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do registro de data e hora é adicionado ao nome do Snapshot.

Opções de retenção de backup

Você pode escolher o número de dias pelos quais deseja manter cópias de backup ou especificar o número de cópias de backup que deseja manter, até um máximo ONTAP de 255 cópias. Por exemplo, sua

organização pode exigir que você mantenha 10 dias de cópias de backup ou 130 cópias de backup.

Ao criar uma política, você pode especificar as opções de retenção para o tipo de backup e o tipo de agendamento.

Se você configurar a replicação do SnapMirror , a política de retenção será espelhada no volume de destino.

O SnapCenter exclui os backups retidos que têm rótulos de retenção que correspondem ao tipo de agendamento. Se o tipo de agendamento foi alterado para o recurso ou grupo de recursos, os backups com o rótulo de tipo de agendamento antigo ainda poderão permanecer no sistema.

Para retenção de cópias de backup a longo prazo, você deve usar o backup SnapVault .

Por quanto tempo manter backups de log de transações no volume de armazenamento de origem para o Exchange Server

O plug-in SnapCenter para Microsoft Exchange Server precisa de backups de log de transações para executar operações de restauração atualizadas, que restauram seu banco de dados para um intervalo entre dois backups completos.

Por exemplo, se o Plug-in for Exchange fizesse um backup completo mais o log de transações às 8h e outro backup completo mais o log de transações às 17h, ele poderia usar o backup mais recente do log de transações para restaurar o banco de dados a qualquer momento entre 8h e 17h. Se os logs de transações não estiverem disponíveis, o Plug-in for Exchange poderá executar apenas operações de restauração pontuais, que restauram um banco de dados para o momento em que o Plug-in for Exchange concluiu um backup completo.

Normalmente, você precisa de operações de restauração atualizadas por apenas um ou dois dias. Por padrão, o SnapCenter retém no mínimo dois dias.

Definir uma estratégia de restauração para bancos de dados do Exchange

Definir uma estratégia de restauração para o Exchange Server permite que você restaure seu banco de dados com sucesso.

Fontes para uma operação de restauração no Exchange Server

Você pode restaurar um banco de dados do Exchange Server a partir de uma cópia de backup no armazenamento primário.

Você pode restaurar bancos de dados somente do armazenamento primário.

Tipos de operações de restauração com suporte para o Exchange Server

Você pode usar o SnapCenter para executar diferentes tipos de operações de restauração em recursos do Exchange.

- Restaurar atualizado
- Restaurar para um ponto anterior no tempo

Restaurar até o minuto

Em uma operação de restauração atualizada, os bancos de dados são recuperados até o ponto de falha. O

SnapCenter faz isso executando a seguinte sequência:

1. Restaura os bancos de dados do backup completo do banco de dados selecionado.
2. Aplica todos os logs de transações que foram copiados, bem como quaisquer novos logs que foram criados desde o backup mais recente.

   Os logs de transações são movidos e aplicados a quaisquer bancos de dados selecionados.

   O Exchange cria uma nova cadeia de logs após a conclusão de uma restauração.

   Melhores práticas: É recomendável que você execute um novo backup completo e de log após a conclusão de uma restauração.

   Uma operação de restauração atualizada requer um conjunto contíguo de logs de transações.

   Após executar uma restauração atualizada, o backup usado para a restauração fica disponível somente para operações de restauração pontuais.

   Se você não precisar manter a capacidade de restauração atualizada para todos os backups, poderá configurar a retenção de backup do log de transações do seu sistema por meio das políticas de backup.

Restaurar para um ponto anterior no tempo

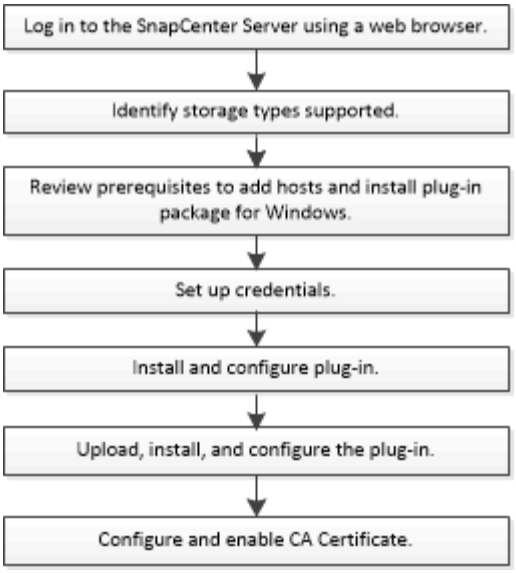
Em uma operação de restauração pontual, os bancos de dados são restaurados apenas para um momento específico do passado. Uma operação de restauração pontual ocorre nas seguintes situações de restauração:

- O banco de dados é restaurado para um determinado momento em um log de transações de backup.
- O banco de dados é restaurado e apenas um subconjunto de logs de transações de backup é aplicado a ele.

Instalar o plug-in SnapCenter para Microsoft Exchange Server

Fluxo de trabalho de instalação do plug-in SnapCenter para Microsoft Exchange Server

Você deve instalar e configurar o SnapCenter Plug-in para Microsoft Exchange Server se quiser proteger bancos de dados do Exchange.



Pré-requisitos para adicionar hosts e instalar o SnapCenter Plug-in para Microsoft Exchange Server

Antes de adicionar um host e instalar os pacotes de plug-in, você deve concluir todos os requisitos.

- Se você estiver usando iSCSI, o serviço iSCSI deverá estar em execução.
- Você deve ter um usuário de domínio com privilégios de administrador local e permissões de login local no host remoto.
- Você deve estar usando o Microsoft Exchange Server 2013, 2016 ou 2019 para configurações autônomas e de Grupo de Disponibilidade de Banco de Dados.
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.
- Se você gerenciar nós de cluster no SnapCenter, deverá ter um usuário com privilégios administrativos para todos os nós do cluster.
- Você deve ter um usuário com permissões administrativas no Exchange Server.
- Se o SnapManager para Microsoft Exchange Server e o SnapDrive para Windows já estiverem instalados, você deverá cancelar o registro do VSS Hardware Provider usado pelo SnapDrive para Windows antes de instalar o Plug-in para Exchange no mesmo Exchange Server para garantir a proteção de dados bem-sucedida usando o SnapCenter.
- Se o SnapManager para Microsoft Exchange Server e o Plug-in para Exchange estiverem instalados no mesmo servidor, você deverá suspender ou excluir do agendador do Windows todos os agendamentos criados pelo SnapManager para Microsoft Exchange Server.
- O host deve ser resolvível para o nome de domínio totalmente qualificado (FQDN) do servidor. Se o arquivo hosts for modificado para torná-lo resolvível e se o nome abreviado e o FQDN forem especificados no arquivo hosts, crie uma entrada no arquivo hosts do SnapCenter no seguinte formato: *<endereço_ip> <fqdn_do_host> <nome_do_host>*.
- Certifique-se de que as seguintes portas não estejam bloqueadas no firewall, caso contrário, a operação de adição de host falhará. Para resolver esse problema, você deve configurar o intervalo de portas dinâmicas. Para obter mais informações, consulte "Documentação da Microsoft" .

- Intervalo de portas 50000 - 51000 para Windows 2016 e Exchange 2016
- Intervalo de portas 6000 - 6500 para Windows 2012 R2 e Exchange 2013
- Intervalo de portas 49152 - 65536 para Windows 2019

Para identificar o intervalo de portas, execute os seguintes comandos:

- netsh int ipv4 mostra porta dinâmica tcp
- netsh int ipv4 mostra porta dinâmica udp
- netsh int ipv6 mostra porta dinâmica tcp
- netsh int ipv6 mostra porta dinâmica udp

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows

Antes de instalar o pacote de plug-ins do SnapCenter para Windows, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas Operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	5 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.

Item	Requisitos
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK O Java 11 Oracle Java e OpenJDK são necessários apenas para SAP HANA, IBM Db2, PostgreSQL, MySQL, plug-ins compatíveis com NetApp e outros aplicativos personalizados que podem ser instalados no host Windows. Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."

Privilégios do Exchange Server necessários

Para permitir que o SnapCenter adicione o Exchange Server ou DAG e instalar o SnapCenter Plug-in para Microsoft Exchange Server em um host ou DAG, você deve configurar o SnapCenter com credenciais para um usuário com um conjunto mínimo de privilégios e permissões.

Você deve ter um usuário de domínio com privilégios de administrador local e com permissões de login local no host remoto do Exchange, bem como permissões administrativas em todos os nós no DAG. O usuário do domínio requer as seguintes permissões mínimas:

- Adicionar-MailboxDatabaseCopy
- Desmontar-Banco de Dados
- Obter-AdServerSettings
- Obter-Grupo de Disponibilidade de Banco de Dados
- Obter-ExchangeServer
- Obter-MailboxDatabase
- Obter-MailboxDatabaseCopyStatus
- Obter-MailboxServer
- Obter-MailboxStatistics
- Obter-PublicFolderDatabase
- Mover-ActiveMailboxDatabase
- Mover-DatabasePath -ConfigurationOnly:$true
- Montar-Banco de Dados

- Novo-MailboxDatabase
- Novo-PublicFolderDatabase
- Remover-MailboxDatabase
- Remover-MailboxDatabaseCopy
- Remover-PublicFolderDatabase
- Currículo-Caixa de CorreioDatabaseCopy
- Definir configurações do servidor de anúncios
- Definir-MailboxDatabase -allowfilerestore:$true
- Definir-MailboxDatabaseCopy
- Definir-PublicFolderDatabase
- Suspender-MailboxDatabaseCopy
- Atualização-MailboxDatabaseCopy

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows

Antes de instalar o pacote de plug-ins do SnapCenter para Windows, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas Operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	5 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.

Item	Requisitos
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK O Java 11 Oracle Java e OpenJDK são necessários apenas para SAP HANA, IBM Db2, PostgreSQL, MySQL, plug-ins compatíveis com NetApp e outros aplicativos personalizados que podem ser instalados no host Windows. Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."

Configurar credenciais para o plug-in SnapCenter para Windows

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter . Você deve criar credenciais para instalar o pacote de plug-in e credenciais adicionais para executar operações de proteção de dados em bancos de dados.

Sobre esta tarefa

Você deve configurar credenciais para instalar plug-ins em hosts Windows. Embora você possa criar credenciais para o Windows após implantar hosts e instalar plug-ins, a prática recomendada é criar credenciais depois de adicionar SVMs, antes de implantar hosts e instalar plug-ins.

Configure as credenciais com privilégios de administrador, incluindo direitos de administrador no host remoto.

Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver privilégios de administrador completos, será necessário atribuir pelo menos os privilégios de grupo de recursos e backup ao nome de usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.

   A janela Credencial é exibida.

4. Na página Credencial, faça o seguinte:

Para este campo…	Faça isso…
Nome da credencial	Digite um nome para a credencial.
Nome de usuário	Digite o nome de usuário usado para autenticação. • Administrador de domínio ou qualquer membro do grupo de administradores Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • Administrador local (somente para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é: `UserName`
Senha	Digite a senha usada para autenticação.
Autenticação	Selecione Windows como o modo de autenticação.

5. Clique em **OK**.

Configurar o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite que você crie uma Conta de Serviço Gerenciada de grupo (gMSA) que fornece gerenciamento automatizado de senhas de contas de serviço a partir de uma conta de domínio gerenciada.

Antes de começar

- Você deve ter um controlador de domínio do Windows Server 2016 ou posterior.
- Você deve ter um host Windows Server 2016 ou posterior, que seja membro do domínio.

Passos

1. Crie uma chave raiz do KDS para gerar senhas exclusivas para cada objeto no seu gMSA.
2. Para cada domínio, execute o seguinte comando no controlador de domínio do Windows: Add-KDSRootKey -EffectiveImmediately
3. Crie e configure seu gMSA:
   a. Crie uma conta de grupo de usuários no seguinte formato:

```
 domainName\accountName$
.. Adicione objetos de computador ao grupo.
.. Use o grupo de usuários que você acabou de criar para criar o
gMSA.
```

   Por exemplo,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correr `Get-ADServiceAccount` comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Habilite o módulo do Active Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando no PowerShell:

```
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. Reinicie seu host.

b. Instale o gMSA no seu host executando o seguinte comando no prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua privilégios administrativos ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no SnapCenter Server.

   O SnapCenter Server instalará os plug-ins selecionados no host e o gMSA especificado será usado como a conta de logon de serviço durante a instalação do plug-in.

Adicionar hosts e instalar o Plug-in para Exchange

Você pode usar a página Adicionar Host do SnapCenter para adicionar hosts do Windows. O Plug-in para Exchange é instalado automaticamente no host especificado. Este é o método recomendado para instalar plug-ins. Você pode adicionar um host e instalar um plug-in para um host individual ou um cluster.

Antes de começar

- Se o sistema operacional do host do SnapCenter Server for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deverá executar o seguinte:
  - Atualize para o Windows Server 2019 (versão do sistema operacional 17763.5936) ou posterior
  - Atualize para o Windows Server 2022 (versão do sistema operacional 20348.2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como o SnapCenter Admin.
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.
- O serviço de enfileiramento de mensagens deve estar em execução.
- Se estiver usando uma conta de serviço gerenciada em grupo (gMSA), você deverá configurar a gMSA com privilégios administrativos. Para obter informações, consulte"Configurar conta de serviço gerenciada de grupo no Windows Server 2016 ou posterior para o Microsoft Exchange Server" .

Sobre esta tarefa

- Não é possível adicionar um SnapCenter Server como um host de plug-in a outro SnapCenter Server.
- Você pode adicionar um host e instalar pacotes de plug-in para um host individual ou um cluster.
- Se um nó de troca fizer parte de um DAG, você não poderá adicionar apenas um nó ao SnapCenter Server.
- Se você estiver instalando plug-ins em um cluster (Exchange DAG), eles serão instalados em todos os nós do cluster, mesmo que alguns nós não tenham bancos de dados em LUNs do NetApp .

A partir do SnapCenter 4.6, o SCE oferece suporte a multilocação e você pode adicionar um host usando os seguintes métodos:

Adicionar operação de host	4.5 e anteriores	4.6 e posterior
Adicionar DAG sem IP em domínios cruzados ou diferentes	Não suportado	Suportado

Adicionar operação de host	4.5 e anteriores	4.6 e posterior
Adicione vários DAGs de IP com nomes exclusivos, residindo no mesmo domínio ou em vários domínios	Suportado	Suportado
Adicionar vários DAGs com ou sem IP que tenham os mesmos nomes de host e/ou nome de banco de dados em domínios cruzados	Não suportado	Suportado
Adicionar vários DAGs IP/sem IP com o mesmo nome e domínio cruzado	Não suportado	Suportado
Adicionar vários hosts autônomos com o mesmo nome e domínio cruzado	Não suportado	Suportado

O plug-in para Exchange depende do pacote de plug-ins do SnapCenter para Windows, e as versões devem ser as mesmas. Durante a instalação do Plug-in para Exchange, o Pacote de Plug-ins do SnapCenter para Windows é selecionado por padrão e é instalado junto com o Provedor de Hardware VSS.

Se o SnapManager para Microsoft Exchange Server e o SnapDrive para Windows já estiverem instalados e você quiser instalar o Plug-in para Exchange no mesmo Exchange Server, será necessário cancelar o registro do VSS Hardware Provider usado pelo SnapDrive para Windows, pois ele é incompatível com o VSS Hardware Provider instalado com o Plug-in para Exchange e o SnapCenter Plug-ins Package para Windows. Para obter mais informações, consulte "Como registrar manualmente o provedor de hardware Data ONTAP VSS" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se **Hosts gerenciados** está selecionado na parte superior.
3. Clique em **Adicionar**.
4. Na página Hosts, faça o seguinte:

Para este campo…	Faça isso…
Tipo de host	Selecione **Windows** como o tipo de host. O SnapCenter Server adiciona o host e então instala no host o Plug-in para Windows e o Plug-in para Exchange, caso ainda não estejam instalados. O plug-in para Windows e o plug-in para Exchange devem ser da mesma versão. Se uma versão diferente do Plug-in para Windows tiver sido instalada anteriormente, o SnapCenter atualizará a versão como parte da instalação.

Para este campo…	Faça isso…
Nome do host	Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o nome de domínio totalmente qualificado (FQDN). Um endereço IP é suportado para hosts de domínio não confiáveis somente se for resolvido para o FQDN. Se você estiver adicionando um host usando o SnapCenter e ele fizer parte de um subdomínio, você deverá fornecer o FQDN. Você pode inserir endereços IP ou o FQDN de um dos seguintes: • Host autônomo • Troca DAG Para um DAG de troca, você pode: ◦ Adicione um DAG fornecendo o nome do DAG, o endereço IP do DAG, o nome do nó ou o endereço IP do nó. ◦ Adicione o cluster DAG sem IP fornecendo o endereço IP ou o FQDN de um dos nós do cluster DAG. ◦ Adicione um DAG sem IP que resida no mesmo domínio ou em um domínio diferente. Você também pode adicionar vários DAGs IP/sem IP com o mesmo nome, mas domínios diferentes. Para um host autônomo ou um Exchange DAG (entre domínios ou mesmo domínio), é recomendável fornecer o FQDN ou o endereço IP do host ou DAG.

Para este campo…	Faça isso…
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte informações sobre como criar uma credencial. Você pode visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou. O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar Host.

5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a serem instalados.

   Quando você seleciona Plug-in para Exchange, o Plug-in SnapCenter para Microsoft SQL Server é desmarcado automaticamente. A Microsoft recomenda que o SQL Server e o Exchange Server não sejam instalados no mesmo sistema devido à quantidade de memória usada e outros recursos exigidos pelo Exchange.

6. (Opcional) Clique em **Mais opções**.

Para este campo…	Faça isso…
Porta	Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.
Caminho de instalação	O caminho padrão é `C:\Program Files\NetApp\SnapCenter`. Opcionalmente, você pode personalizar o caminho.
Adicionar todos os hosts no DAG	Marque esta caixa de seleção ao adicionar um DAG.

Para este campo…	Faça isso…
Ignorar verificações de pré-instalação	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.
Use a conta de serviço gerenciada em grupo (gMSA) para executar os serviços do plug-in	Marque esta caixa de seleção se desejar usar a Conta de Serviço Gerenciada em Grupo (gMSA) para executar os serviços do plug-in. Forneça o nome do gMSA no seguinte formato: *domainName\accountName$*. O gMSA será usado como uma conta de serviço de logon somente para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

   Se você não tiver marcado a caixa de seleção Ignorar pré-verificações, o host será validado para determinar se atende aos requisitos para instalar o plug-in. Se os requisitos mínimos não forem atendidos, as mensagens de erro ou aviso apropriadas serão exibidas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em `C:\Program Files\NetApp\SnapCenter` WebApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, deverá atualizar o arquivo em ambos os nós.

8. Monitore o progresso da instalação.

Configurar porta personalizada para comunicação NET TCP

Por padrão, a partir da versão 6.0 do SnapCenter , o plug-in SnapCenter para Windows usa a porta 909 para comunicação NET TCP. Se a porta 909 estiver em uso, você pode configurar outra porta para comunicação NET TCP.

Passos

1. Modifique o valor da chave *NetTCPPort* localizada em *C:\Program Files\ NetApp\ SnapCenter\ SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe.config* para o número de porta necessário.
   `<add key="NetTCPPort" value="new_port_number" />`
2. Modifique o valor da chave *NetTCPPort* localizada em *C:\Program Files\ NetApp\ SnapCenter\ SnapCenter Plug-in for Microsoft Windows\SnapDriveService.dll.config* para o número de porta necessário.
   `<add key="NetTCPPort" value="new_port_number" />`
3. Cancele o registro do serviço *Data ONTAP VSS Hardware Provider* executando o comando abaixo:
   `"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\navssprv.exe" -r service -u`

Verifique se o serviço não está sendo exibido na lista de serviços em *services.msc*.

4. Registre o serviço *Data ONTAP VSS Hardware Provider* executando o comando abaixo:
   `"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"`

   Verifique se o serviço agora é exibido na lista de serviços em *services.msc*.

5. Reinicie o serviço *Plug-in para Windows*.

Instalar o Plug-in para Exchange do host do SnapCenter Server usando cmdlets do PowerShell

Você deve instalar o Plug-in para Exchange a partir da GUI do SnapCenter . Se não quiser usar a GUI, você pode usar cmdlets do PowerShell no host do SnapCenter Server ou em um host remoto.

Antes de começar

- O SnapCenter Server deve ter sido instalado e configurado.
- Você deve ser um administrador local no host ou um usuário com privilégios administrativos.
- Você deve ser um usuário atribuído a uma função que tenha permissões de plug-in, instalação e desinstalação, como o SnapCenter Admin.
- Você deve ter revisado os requisitos de instalação e os tipos de configurações suportadas antes de instalar o Plug-in para Exchange.
- O host no qual você deseja instalar o Plug-in para Exchange deve ser um host Windows.

Passos

1. No host do SnapCenter Server, estabeleça uma sessão usando o cmdlet *Open-SmConnection* e insira suas credenciais.
2. Adicione o host no qual você deseja instalar o Plug-in para Exchange usando o cmdlet *Add-SmHost* com os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

   O host pode ser um host autônomo ou um DAG. Se você especificar um DAG, o parâmetro *-IsDAG* será necessário.

3. Instale o Plug-in para Exchange usando o cmdlet *Install-SmHostPackage* com os parâmetros necessários.

   Este comando instala o Plug-in para Exchange no host especificado e, em seguida, registra o plug-in no SnapCenter.

Instalar o plug-in SnapCenter para Exchange silenciosamente a partir da linha de comando

Você deve instalar o Plug-in for Exchange a partir da interface do usuário do SnapCenter . Entretanto, se por algum motivo você não puder, você pode executar o programa de

instalação do Plug-in for Exchange de forma autônoma no modo silencioso a partir da linha de comando do Windows.

Antes de começar

- Você deve ter feito backup dos recursos do Microsoft Exchange Server.
- Você deve ter instalado os pacotes de plug-in do SnapCenter .
- Você deve excluir a versão anterior do SnapCenter Plug-in para Microsoft SQL Server antes de instalar.

  Para obter mais informações, consulte "Como instalar um plug-in SnapCenter manualmente e diretamente do host do plug-in" .

Passos

1. Valide se a pasta *C:\temp* existe no host do plug-in e se o usuário conectado tem acesso total a ela.
2. Baixe o plug-in SnapCenter para Microsoft Windows em *C:\ProgramData\ NetApp\ SnapCenter\Package* Repository.

   Este caminho pode ser acessado a partir do host onde o SnapCenter Server está instalado.
3. Copie o arquivo de instalação para o host no qual você deseja instalar o plug-in.
4. Em um prompt de comando do Windows no host local, navegue até o diretório onde você salvou os arquivos de instalação do plug-in.
5. Digite o seguinte comando para instalar o plug-in.

   snapcenter_windows_host_plugin.exe"/silent /debuglog"<Caminho_do_Log_de_Depuração>" /log"<Caminho_do_Log>" BI_SNAPCENTER_PORT=<Num> SUITE_INSTALLDIR="<Caminho_do_Diretório_de_Instalação>" BI_SERVICEACCOUNT=<domínio\administrador> BI_SERVICEPWD=<senha> ISFeatureInstall=HPPW,SCW,SCE

   Por exemplo:

   C:\ProgramData\ NetApp\ SnapCenter\Repositório de pacotes\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\temp" BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR="C:\Arquivos de programas\ NetApp\ SnapCenter" BI_SERVICEACCOUNT=domínio\administrador BI_SERVICEPWD=senha ISFeatureInstall=HPPW,SCW,SCE

   Todos os parâmetros passados durante a instalação do Plug-in for Exchange diferenciam maiúsculas de minúsculas.

   Insira os seguintes valores para as variáveis:

Variável	Valor
/debuglog"<Caminho_do_Log_de_Depuração>	Especifique o nome e o local do arquivo de log do instalador do pacote, como no exemplo a seguir: *Setup.exe /debuglog"C:\CaminhoParaLog\setupexe.log*

Variável	Valor
PORTA_BI_SNAPCENTER	Especifique a porta na qual o SnapCenter se comunica com o SMCore.
SUITE_INSTALLDIR	Especifique o diretório de instalação do pacote de plug-in do host.
CONTA_DE_SERVIÇO_BI	Especifique o plug-in SnapCenter para a conta de serviço web do Microsoft Windows.
BI_SERVICEPWD	Especifique a senha para a conta de serviço web do SnapCenter Plug-in para Microsoft Windows.
Instalação do ISFeature	Especifique a solução a ser implantada pelo SnapCenter no host remoto.

6. Monitore o agendador de tarefas do Windows, o arquivo de log de instalação principal *C:\Installdebug.log* e os arquivos de instalação adicionais em *C:\Temp*.
7. Monitore o diretório *%temp%* para verificar se os instaladores *msiexe.exe* estão instalando o software sem erros.

A instalação do Plug-in for Exchange registra o plug-in no host e não no SnapCenter Server. Você pode registrar o plug-in no SnapCenter Server adicionando o host usando a GUI do SnapCenter ou o cmdlet do PowerShell. Depois que o host é adicionado, o plug-in é descoberto automaticamente.

Monitorar o status de instalação do pacote de plug-in SnapCenter

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.

3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
   a. Clique em **Filtrar**.
   b. Opcional: especifique a data de início e término.
   c. No menu suspenso Tipo, selecione **Instalação de plug-in**.
   d. No menu suspenso Status, selecione o status da instalação.
   e. Clique em **Aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Configurar certificado CA

Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.

O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte "Como gerar um arquivo CSR de certificado CA" .

Se você possui o certificado CA para seu domínio (*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.

5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Importar chave privada	Selecione a opção **Sim**, importe a chave privada e clique em **Avançar**.
Formato de arquivo de importação	Não faça alterações; clique em **Avançar**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

> O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: *.pfx, *.p12 e *.p7b).

7. Repita a Etapa 5 para a pasta “Pessoal”.

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

Passos

1. Execute o seguinte na GUI:
   a. Clique duas vezes no certificado.
   b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.
   c. Percorra a lista de campos e clique em **Impressão digital**.
   d. Copie os caracteres hexadecimais da caixa.
   e. Remova os espaços entre os números hexadecimais.

      Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
   a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copie a impressão digital.

Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Por exemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Vincule o certificado recém-instalado aos serviços de plug-in do host
   do Windows, executando os seguintes comandos:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Por exemplo:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *Get-SmCertificateSettings*.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- *  * indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- *  * indica que o certificado CA foi validado com sucesso.
- *  * indica que o certificado CA não pôde ser validado.
- *  * indica que as informações de conexão não puderam ser recuperadas.

Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Configurar o SnapManager 7.x para que o Exchange e o SnapCenter coexistam

Para permitir que o SnapCenter Plug-in para Microsoft Exchange Server coexista com o SnapManager para Microsoft Exchange Server, você precisa instalar o SnapCenter Plug-in para Microsoft Exchange Server no mesmo Exchange Server em que o SnapManager para Microsoft Exchange Server está instalado, desabilitar os agendamentos do SnapManager para Exchange e configurar novos agendamentos e backups usando o SnapCenter Plug-in para Microsoft Exchange Server.

Antes de começar

- O SnapManager para Microsoft Exchange Server e o SnapDrive para Windows já estão instalados, e os backups do SnapManager para Microsoft Exchange Server existem no sistema e no diretório SnapInfo.
- Você deve ter excluído ou recuperado os backups feitos pelo SnapManager para Microsoft Exchange Server dos quais não precisa mais.
- Você deve ter suspendido ou excluído todos os agendamentos criados pelo SnapManager para Microsoft Exchange Server do agendador do Windows.
- O SnapCenter Plug-in para Microsoft Exchange Server e o SnapManager para Microsoft Exchange Server podem coexistir no mesmo Exchange Server, mas você não pode atualizar instalações existentes do SnapManager para Microsoft Exchange Server para o SnapCenter.

  O SnapCenter não oferece uma opção para atualização.

- O SnapCenter não oferece suporte à restauração de bancos de dados do Exchange a partir do SnapManager para backup do Microsoft Exchange Server.

  Se você não desinstalar o SnapManager para Microsoft Exchange Server após a instalação do SnapCenter Plug-in para Microsoft Exchange Server e depois quiser restaurar um backup do SnapManager para Microsoft Exchange Server, será necessário executar etapas adicionais.

Passos

1. Usando o PowerShell em todos os nós DAG, determine se o SnapDrive para Windows VSS Hardware Provider está registrado: *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. No diretório SnapDrive , cancele o registro do VSS Hardware Provider do SnapDrive para Windows: *navssprv.exe -r service –u*
3. Verifique se o VSS Hardware Provider foi removido: *vssadmin list providers*
4. Adicione o host do Exchange ao SnapCenter e instale o SnapCenter Plug-in para Microsoft Windows e o SnapCenter Plug-in para Microsoft Exchange Server.
5. No diretório do plug-in SnapCenter para Microsoft Windows em todos os nós DAG, verifique se o provedor de hardware VSS está registrado: *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. Interrompa os agendamentos de backup do SnapManager para Microsoft Exchange Server.
7. Usando a GUI do SnapCenter , crie backups sob demanda, configure backups agendados e defina configurações de retenção.
8. Desinstale o SnapManager para Microsoft Exchange Server.

   Se você não desinstalar o SnapManager para Microsoft Exchange Server agora e quiser restaurar um backup do SnapManager para Microsoft Exchange Server mais tarde:

   a. Cancelar o registro do SnapCenter Plug-in para Microsoft Exchange Server de todos os nós DAG: *navssprv.exe -r service -u*

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
Windows>navssprv.exe -r service -u
```

b. No diretório *C:\Program Files\ NetApp\ SnapDrive*, registre o SnapDrive para Windows em todos os nós DAG: *navssprv.exe -r service -a hostname\\username -p password*

Instalar o SnapCenter Plug-in for VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs), ou se você quiser proteger VMs e armazenamentos de dados, será necessário implantar o SnapCenter Plug-in for VMware vSphere .

Para obter informações sobre como implantar, consulte "Visão geral da implantação" .

Implantar certificado CA

Para configurar o Certificado CA com o SnapCenter Plug-in for VMware vSphere, consulte "Criar ou importar certificado SSL" .

Configurar o arquivo CRL

O SnapCenter Plug-in for VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL do SnapCenter Plug-in for VMware vSphere é */opt/netapp/config/crl*.

Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Prepare-se para a proteção de dados

Antes de executar qualquer operação de proteção de dados, como operações de backup, clonagem ou restauração, você deve definir sua estratégia e configurar o ambiente. Você também pode configurar o SnapCenter Server para usar a tecnologia SnapMirror e SnapVault .

Para aproveitar a tecnologia SnapVault e SnapMirror , você deve configurar e inicializar um relacionamento de proteção de dados entre os volumes de origem e destino no dispositivo de armazenamento. Você pode usar o NetAppSystem Manager ou usar a linha de comando do console de armazenamento para executar essas tarefas.

Encontre mais informações

"Introdução à API REST"

Pré-requisitos para usar o plug-in SnapCenter para Microsoft Exchange Server

Antes de usar o Plug-in para Exchange, o administrador do SnapCenter deve instalar e configurar o SnapCenter Server e executar as tarefas de pré-requisito.

- Instalar e configurar o SnapCenter Server.

- Efetue login no SnapCenter.
- Configure o ambiente SnapCenter adicionando ou atribuindo conexões do sistema de armazenamento e criando uma credencial.

  O SnapCenter não oferece suporte a várias SVMs com o mesmo nome em clusters diferentes. Cada SVM suportado pelo SnapCenter deve ter um nome exclusivo.

- Adicione hosts, instale o SnapCenter Plug-in para Microsoft Windows e o SnapCenter Plug-in para Microsoft Exchange Server e descubra (atualize) os recursos.
- Execute o provisionamento de armazenamento do lado do host usando o plug-in SnapCenter para Microsoft Windows.
- Se você estiver usando o SnapCenter Server para proteger bancos de dados do Exchange que residem em LUNs do VMware RDM, será necessário implantar o SnapCenter Plug-in for VMware vSphere e registrar o plug-in no SnapCenter. A documentação do SnapCenter Plug-in for VMware vSphere tem mais informações.

  VMDKs não são suportados.

- Mova um banco de dados existente do Microsoft Exchange Server de um disco local para um armazenamento compatível usando ferramentas do Microsoft Exchange.
- Configure relacionamentos SnapMirror e SnapVault , se desejar replicação de backup.

Para usuários do SnapCenter 4.1.1, a documentação do SnapCenter Plug-in for VMware vSphere 4.1.1 contém informações sobre como proteger bancos de dados e sistemas de arquivos virtualizados. Para usuários do SnapCenter 4.2.x, a documentação do NetApp Data Broker 1.0 e 1.0.1 contém informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o SnapCenter Plug-in for VMware vSphere fornecido pelo dispositivo virtual NetApp Data Broker baseado em Linux (formato Open Virtual Appliance). Para usuários do SnapCenter 4.3.x, a documentação do SnapCenter Plug-in for VMware vSphere 4.3 contém informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o dispositivo virtual SnapCenter Plug-in for VMware vSphere baseado em Linux (formato Open Virtual Appliance).

"Documentação do SnapCenter Plug-in for VMware vSphere"

Como recursos, grupos de recursos e políticas são usados para proteger o Exchange Server

Antes de usar o SnapCenter, é útil entender os conceitos básicos relacionados às operações de backup, restauração e redefinição que você deseja executar. Você interage com recursos, grupos de recursos e políticas para diferentes operações.

- Os recursos geralmente são bancos de dados de caixa de correio ou Grupo de Disponibilidade de Banco de Dados (DAG) do Microsoft Exchange dos quais você faz backup com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host ou Exchange DAG, e o grupo de recursos pode incluir um DAG inteiro ou bancos de dados individuais.

  Ao executar uma operação em um grupo de recursos, você executa essa operação nos recursos definidos no grupo de recursos de acordo com o cronograma especificado para o grupo de recursos.

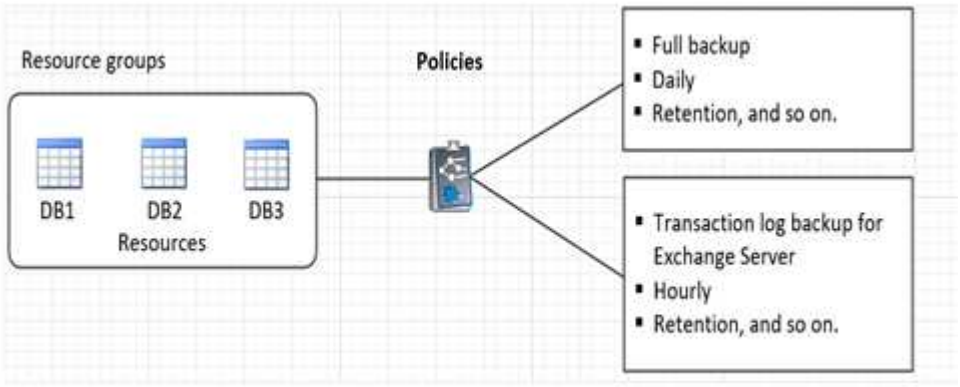
  Você pode fazer backup sob demanda de um único recurso ou de um grupo de recursos. Você também pode executar backups agendados para recursos individuais e grupos de recursos.

Os grupos de recursos eram anteriormente conhecidos como conjuntos de dados.

- As políticas especificam a frequência de backup, retenção de cópias, scripts e outras características das operações de proteção de dados.

  Ao criar um grupo de recursos, você seleciona uma ou mais políticas para esse grupo. Você também pode selecionar uma ou mais políticas ao executar um backup sob demanda para um único recurso.

Pense em um grupo de recursos como definidor de *o que* você quer proteger e quando quer proteger em termos de dia e hora. Pense em uma política como a definição de *como* você quer protegê-la. Se você estiver fazendo backup de todos os bancos de dados de um host, por exemplo, poderá criar um grupo de recursos que inclua todos os bancos de dados no host. Você pode então anexar duas políticas ao grupo de recursos: uma política diária e uma política horária. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diariamente e outra programação que executa backups de log a cada hora. A imagem a seguir ilustra o relacionamento entre recursos, grupos de recursos e políticas para bancos de dados:



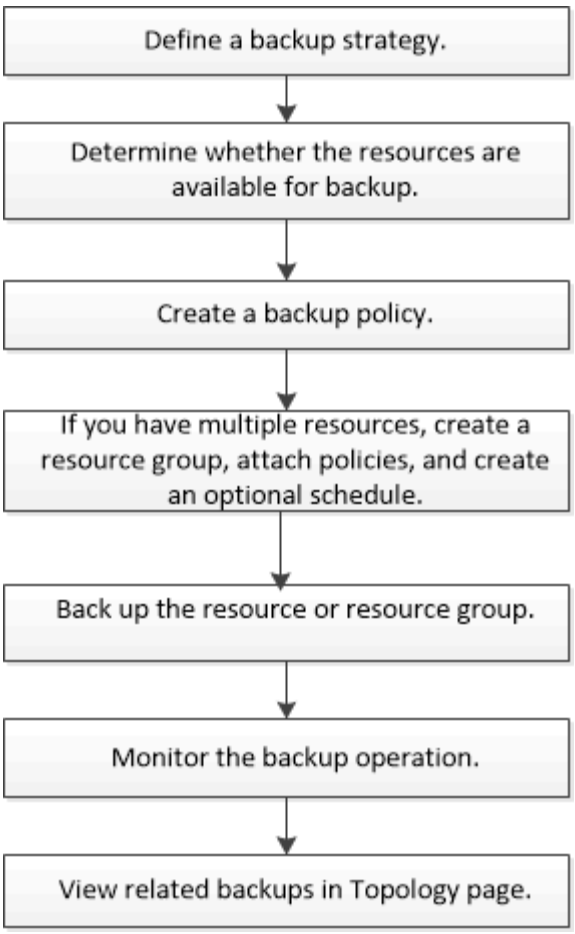
Fazer backup dos recursos do Exchange

Fluxo de trabalho de backup

Ao instalar o SnapCenter Plug-in para Microsoft Exchange Server em seu ambiente, você pode usar o SnapCenter para fazer backup de recursos do Exchange.

Você pode agendar vários backups para serem executados em todos os servidores simultaneamente. As operações de backup e restauração não podem ser executadas simultaneamente no mesmo recurso. Cópias de backup ativas e passivas no mesmo volume não são suportadas.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de backup:



Banco de dados de troca e verificação de backup

O plug-in SnapCenter para Microsoft Exchange Server não fornece verificação de backup; no entanto, você pode usar a ferramenta Eseutil fornecida com o Exchange para verificar bancos de dados e backups do Exchange.

A ferramenta Microsoft Exchange Eseutil é um utilitário de linha de comando incluído no seu servidor Exchange. O utilitário permite que você execute verificações de consistência para verificar a integridade dos bancos de dados e backups do Exchange.

Melhores práticas: Não é necessário executar verificações de consistência em bancos de dados que fazem parte de uma configuração de Grupo de Disponibilidade de Banco de Dados (DAG) com pelo menos duas réplicas.

Para obter informações adicionais, consulte "Documentação do Microsoft Exchange Server" .

Determinar se os recursos do Exchange estão disponíveis para backup

Os recursos são os bancos de dados, Grupos de Disponibilidade de Banco de Dados do Exchange que são mantidos pelos plug-ins que você instalou. Você pode adicionar esses recursos a grupos de recursos para poder executar tarefas de proteção de dados, mas primeiro você deve identificar quais recursos estão disponíveis. Determinar os recursos disponíveis também verifica se a instalação do plug-in foi concluída com sucesso.

Antes de começar

- Você já deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts, criar conexões de sistema de armazenamento, adicionar credenciais e instalar o Plug-in para Exchange.
- Para aproveitar os recursos do software Single Mailbox Recovery, você deve ter localizado seu banco de dados ativo no Exchange Server onde o software Single Mailbox Recovery está instalado.
- Se os bancos de dados residirem em LUNs do VMware RDM, você deverá implantar o SnapCenter Plug-in for VMware vSphere e registrar o plug-in no SnapCenter. O "Documentação do SnapCenter Plug-in for VMware vSphere" tem mais informações.

Sobre esta tarefa

- Não é possível fazer backup de bancos de dados quando a opção **Status geral** na página Detalhes estiver definida como Não disponível para backup. A opção **Status geral** é definida como Não disponível para backup quando qualquer uma das seguintes condições for verdadeira:
  - Os bancos de dados não estão em um LUN do NetApp .
  - Os bancos de dados não estão em estado normal.

    Os bancos de dados não estão em estado normal quando estão em estado de montagem, desmontagem, nova propagação ou recuperação pendente.
- Se você tiver um Grupo de Disponibilidade de Banco de Dados (DAG), poderá fazer backup de todos os bancos de dados do grupo executando a tarefa de backup no DAG.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione **Microsoft Exchange Server** na lista suspensa de plug-ins localizada no canto superior esquerdo da página Recursos.
2. Na página Recursos, selecione **Banco de dados**, ou **Grupo de disponibilidade de banco de dados**, ou **Grupo de recursos**, na lista suspensa **Exibir**.

   Todos os bancos de dados e DAGs são exibidos com seus DAGs ou nomes de host no formato FQDN, para que você possa distinguir entre vários bancos de dados.

   Clique e selecione o nome do host e o Exchange Server para filtrar os recursos. Você pode então clicar para fechar o painel de filtro.
3. Clique em **Atualizar recursos**.

   Os recursos recém-adicionados, renomeados ou excluídos são atualizados para o inventário do SnapCenter Server.

   > Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

   Os recursos são exibidos junto com informações como nome do recurso, nome do grupo de disponibilidade do banco de dados, servidor no qual o banco de dados está ativo no momento, servidor com cópias, hora do último backup e status geral.

   - Se o banco de dados estiver em um armazenamento não NetApp , Não disponível para backup será exibido na coluna Status geral.

     Em um DAG, se a cópia ativa do banco de dados estiver em um armazenamento não NetApp e se pelo menos uma cópia passiva do banco de dados estiver em um armazenamento NetApp , Não protegido será exibido na coluna **Status geral**.

Não é possível executar operações de proteção de dados em um banco de dados que esteja em um tipo de armazenamento que não seja NetApp .

- Se o banco de dados estiver no armazenamento NetApp e não estiver protegido, Não protegido será exibido na coluna **Status geral**.
- Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, a interface do usuário exibirá a mensagem Backup não executado na coluna **Status geral**.
- Se o banco de dados estiver em um sistema de armazenamento NetApp e estiver protegido, e se o backup for acionado para o banco de dados, a interface do usuário exibirá a mensagem Backup bem-sucedido na coluna **Status geral**.

Criar políticas de backup para bancos de dados do Exchange Server

Você pode criar uma política de backup para os recursos do Exchange ou para os grupos de recursos antes de usar o SnapCenter para fazer backup dos recursos do Microsoft Exchange Server ou pode criar uma política de backup no momento em que cria um grupo de recursos ou faz backup de um único recurso.

Antes de começar

- Você deve ter definido sua estratégia de proteção de dados.

  Para obter detalhes, consulte as informações sobre como definir uma estratégia de proteção de dados para bancos de dados do Exchange.

- Você deve estar preparado para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, identificar recursos e criar conexões de sistema de armazenamento.
- Você deve ter atualizado (descoberto) os recursos do Exchange Server.
- Se você estiver replicando Snapshots para um espelho ou cofre, o administrador do SnapCenter deverá ter atribuído as máquinas virtuais de armazenamento (SVMs) para os volumes de origem e de destino a você.
- Se você quiser executar os scripts do PowerShell em prescrições e postscripts, você deve definir o valor do `usePowershellProcessforScripts` parâmetro para verdadeiro no `web.config` arquivo.

  O valor padrão é falso.

- Revise os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror . Para obter informações, consulte "Limites de objetos para sincronização ativa do SnapMirror" .

Sobre esta tarefa

- Uma política de backup é um conjunto de regras que rege como você gerencia e mantém backups e com que frequência o recurso ou grupo de recursos é feito backup. Além disso, você pode especificar configurações de script. Especificar opções em uma política economiza tempo quando você deseja reutilizar a política para outro grupo de recursos.
- A retenção de backup completo é específica para uma determinada política. Um banco de dados ou recurso que usa a política A com uma retenção de backup completo de 4 retém 4 backups completos e não tem efeito na política B para o mesmo banco de dados ou recurso, que pode ter uma retenção de 3 para reter 3 backups completos.
- A retenção de backup de log é eficaz em todas as políticas e se aplica a todos os backups de log de um banco de dados ou recurso. Portanto, quando um backup completo é executado usando a política B, a configuração de retenção de log afeta os backups de log criados pela política A no mesmo banco de

dados ou recurso. Da mesma forma, a configuração de retenção de log para a política A afeta os backups de log criados pela política B no mesmo banco de dados.

- O SCRIPTS_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCoreServiceHost.exe.Config do host do plug-in.

  Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável que você use o caminho padrão por segurança.

  O valor da chave pode ser exibido no swagger por meio da API: API /4.7/configsettings

  Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

  Melhores práticas: É melhor configurar a política de retenção secundária com base no número geral de backups completos e de log que você deseja manter. Ao configurar políticas de retenção secundárias, lembre-se de que, quando os bancos de dados e logs estão em volumes diferentes, cada backup pode ter três Snapshots e, quando os bancos de dados e logs estão no mesmo volume, cada backup pode ter dois Snapshots.

- SnapLock

  - Se a opção 'Manter as cópias de backup por um número específico de dias' for selecionada, o período de retenção do SnapLock deverá ser menor ou igual aos dias de retenção mencionados.

    Especificar um período de bloqueio de Snapshot impede a exclusão dos Snapshots até que o período de retenção expire. Isso pode levar à retenção de um número maior de Snapshots do que a contagem especificada na política.

  Para versões do ONTAP 9.12.1 e anteriores, os clones criados a partir dos SnapLock Vault Snapshots herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Clique em **Novo**.
4. Na página Nome, insira o nome e os detalhes da política.
5. Na página Tipo de backup e replicação, execute as seguintes etapas:

   a. Escolha o tipo de backup:

Se você quiser…	Faça isso…
Faça backup dos arquivos do banco de dados e dos logs de transações necessários	Selecione **Backup completo e Backup de log**. Os bancos de dados são copiados com truncamento de log, e todos os logs são copiados, incluindo os logs truncados. Este é o tipo de backup recomendado.

Se você quiser…	Faça isso…
Faça backup dos arquivos do banco de dados e dos logs de transações não confirmados	Selecione **Backup completo**. Os bancos de dados são copiados com truncamento de log, e logs truncados não são copiados.
Faça backup de todos os logs de transações	Selecione **Backup de log**. Todos os logs de transações no sistema de arquivos ativo são copiados e não há truncamento de log. Um diretório *scebackupinfo* é criado no mesmo disco que o log ativo. Este diretório contém o ponteiro para as alterações incrementais do banco de dados do Exchange e não é equivalente aos arquivos de log completos.
Faça backup de todos os arquivos de banco de dados e logs de transações sem truncar os arquivos de log de transações	Selecione **Copiar backup**. Todos os bancos de dados e todos os logs são copiados e não há truncamento de logs. Normalmente, você usa esse tipo de backup para repropagar uma réplica ou para testar ou diagnosticar um problema.

Você deve definir o espaço necessário para backups de log com base na retenção de backup completa e não com base na retenção atualizada (UTM).

Crie políticas de cofre separadas para logs e bancos de dados ao lidar com volumes do Exchange (LUNs) e defina a retenção (keep) da política de log como o dobro do número para cada rótulo da política de banco de dados, usando os mesmos rótulos. Para mais informações, veja, "Os backups do SnapCenter for Exchange mantêm apenas metade dos instantâneos no volume de log de destino do Vault"

b. Na seção Configurações do Grupo de Disponibilidade do Banco de Dados, selecione uma ação:

Para este campo…	Faça isso…
Fazer backup de cópias ativas	Selecione esta opção para fazer backup somente das cópias ativas do banco de dados selecionado. Para grupos de disponibilidade de banco de dados (DAGs), esta opção faz backup apenas de cópias ativas de todos os bancos de dados no DAG. Cópias passivas não são feitas backup.

Para este campo…	Faça isso…
Faça cópias de backup em servidores a serem selecionados no momento da criação do trabalho de backup	Selecione esta opção para fazer backup de quaisquer cópias dos bancos de dados nos servidores selecionados, tanto ativos quanto passivos. Para DAGs, esta opção faz backup de cópias ativas e passivas de todos os bancos de dados nos servidores selecionados.

Em configurações de cluster, os backups são retidos em cada nó do cluster de acordo com as configurações de retenção definidas na política. Se o nó proprietário do cluster for alterado, os backups do nó proprietário anterior serão mantidos. A retenção é aplicável somente no nível do nó.

c. Na seção Frequência da programação, selecione um ou mais tipos de frequência: **Sob demanda**, **Por hora**, **Diária**, **Semanal** e **Mensal**.

Você pode especificar o agendamento (data de início, data de término) para operações de backup ao criar um grupo de recursos. Isso permite que você crie grupos de recursos que compartilham a mesma política e frequência de backup, mas permite que você atribua agendamentos de backup diferentes a cada política.

Se você agendou para 2h00, a programação não será acionada durante o horário de verão (DST).

a. Selecione o rótulo Política.

Você pode atribuir rótulos SnapMirror a snapshots primários para replicação remota, permitindo que os snapshots primários descarreguem a operação de replicação de snapshots do SnapCenter para sistemas secundários ONTAP . Isso pode ser feito sem habilitar a opção SnapMirror ou SnapVault na página de política.

b. Na seção Selecionar opções de replicação secundária, selecione uma ou ambas as seguintes opções de replicação secundária:

Para este campo…	Faça isso…
Atualizar o SnapMirror após criar um Snapshot local	Selecione esta opção para manter cópias espelhadas de conjuntos de backup em outro volume (SnapMirror). Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Esta opção deve ser habilitada para sincronização ativa do SnapMirror . A política somente primária não pode ser usada se a sincronização ativa do SnapMirror estiver configurada para volumes do Exchange ONTAP . O SnapCenter não permite isso. Você deve habilitar a opção "Espelho". Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Ver "Exibir backups do Exchange na página Topologia" .
Atualizar o SnapVault após criar um Snapshot local	Selecione esta opção para executar a replicação de backup de disco para disco.
Contagem de novas tentativas de erro	Insira o número de tentativas de replicação que devem ocorrer antes que o processo seja interrompido.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o armazenamento secundário para evitar atingir o limite máximo de Snapshots no armazenamento secundário.

6. Na página Retenção, configure as definições de retenção.

   As opções exibidas dependem do tipo de backup e do tipo de frequência selecionados anteriormente.

O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida como um valor maior do que o suportado pela versão subjacente do ONTAP .

Você deve definir a contagem de retenção como 2 ou mais se planeja habilitar a replicação do SnapVault . Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro Snapshot será o Snapshot de referência para o relacionamento SnapVault até que um Snapshot mais recente seja replicado para o destino.

a. Na seção Configurações de retenção de backups de log, selecione uma das seguintes opções:

Se você quiser…	Faça isso…
Manter apenas um número específico de backups de log	Selecione **Número de backups completos para os quais os logs são retidos** e especifique o número de backups completos para os quais você deseja restauração atualizada. A retenção atualizada (UTM) se aplica ao backup de log criado por meio de backup completo ou de log. Por exemplo, se as configurações de retenção de UTM estiverem configuradas para reter backups de log dos últimos 5 backups completos, os backups de log dos últimos 5 backups completos serão retidos. As pastas de log criadas como parte de backups completos e de log são excluídas automaticamente como parte do UTM. Você não pode excluir as pastas de log manualmente. Por exemplo, se a configuração de retenção de backup completo ou completo e de log for definida para 1 mês e a retenção UTM for definida para 10 dias, a pasta de log criada como parte desses backups será excluída conforme UTM. Como resultado, apenas as pastas de log de 10 dias estarão lá e todos os outros backups serão marcados para restauração em um determinado momento. Você pode definir o valor de retenção UTM como 0, se não quiser executar uma restauração atualizada. Isso permitirá a operação de restauração em um determinado momento. **Melhores práticas:** é melhor que a configuração seja igual à configuração de Total Snapshots (backups completos) na seção Configurações de retenção de backup completo. Isso garante que os arquivos de log sejam mantidos para cada backup completo.
Manter as cópias de segurança por um número específico de dias	Selecione a opção **Manter backups de log para o último** e especifique o número de dias para manter as cópias de backup de log. Os backups de log até o número de dias de backups completos são mantidos.

Se você quiser…	Faça isso…
Período de bloqueio de instantâneo	Selecione **Período de bloqueio de cópia de instantâneo** e selecione dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

Se você selecionou **Backup de log** como o tipo de backup, os backups de log serão retidos como parte das configurações de retenção atualizadas para backups completos.

b. Na seção Configurações de retenção de backup completo, selecione uma das seguintes opções para backups sob demanda e, em seguida, selecione uma para backups completos:

Para este campo…	Faça isso…
Manter apenas um número específico de Snapshots	Se você quiser especificar o número de backups completos a serem mantidos, selecione a opção **Total de cópias de instantâneos a serem mantidas** e especifique o número de instantâneos (backups completos) a serem mantidos. Se o número de backups completos exceder o número especificado, os backups completos que excederem o número especificado serão excluídos, com as cópias mais antigas sendo excluídas primeiro.
Manter backups completos por um número específico de dias	Selecione a opção **Manter cópias de instantâneos por** e especifique o número de dias para manter os instantâneos (backups completos).
Período de bloqueio do instantâneo primário	Selecione **Período de bloqueio de cópia do instantâneo primário** e selecione dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.
Período de bloqueio do instantâneo secundário	Selecione **Período de bloqueio de cópia de instantâneo secundário** e selecione dias, meses ou anos.

Se você tiver um banco de dados com apenas backups de log e nenhum backup completo em um host em uma configuração DAG, os backups de log serão mantidos das seguintes maneiras:

- Por padrão, o SnapCenter encontra o backup completo mais antigo para esse banco de dados em todos os outros hosts no DAG e exclui todos os backups de log nesse host que foram feitos antes do backup completo.

- Você pode substituir o comportamento de retenção padrão acima para um banco de dados em um host em um DAG com apenas backups de log adicionando a chave **MaxLogBackupOnlyCountWithoutFullBackup** no arquivo *C:\Program Files\ NetApp\ SnapCenter WebApp\web.config*.

  ```
  <add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
  ```

  No exemplo, o valor 10 significa que você mantém até 10 backups de log no host.

7. Na página Script, insira o caminho e os argumentos do prescript ou postscript que devem ser executados antes ou depois da operação de backup, respectivamente.
   - Os argumentos de backup prescritos incluem “$Database” e “$ServerInstance”.
   - Os argumentos de backup do Postscript incluem “$Database”, “$ServerInstance”, “$BackupName”, “$LogDirectory” e “$LogSnapshot”.

     Você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.

   O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_PATH.

8. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas para servidores Exchange

Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que deseja executar e o cronograma de proteção.

Sobre esta tarefa

- O SCRIPTS_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCoreServiceHost.exe.Config do host do plug-in.

  Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável que você use o caminho padrão por segurança.

  O valor da chave pode ser exibido no swagger por meio da API: API /4.7/configsettings

  Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .
- Não há suporte para adicionar novos bancos de dados sem sincronização ativa do SnapMirror a um grupo de recursos existente que contém recursos com sincronização ativa do SnapMirror .
- Não há suporte para adicionar novos bancos de dados a um grupo de recursos existente no modo de failover da sincronização ativa do SnapMirror . Você pode adicionar recursos ao grupo de recursos somente no estado regular ou de failback.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in do Microsoft Exchange Server na lista.
2. Na página Recursos, selecione **Banco de dados** na lista **Exibir**.

   Se você adicionou recentemente um recurso ao SnapCenter, clique em **Atualizar recursos** para visualizar o recurso recém-adicionado.

3. Clique em **Novo Grupo de Recursos**.
4. Na página Nome, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Digite o nome do grupo de recursos. O nome do grupo de recursos não deve exceder 250 caracteres.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.
Use formato de nome personalizado para cópia do Snapshot	Opcional: insira um nome e formato de Snapshot personalizado. Por exemplo, *customtext_resourcegroup_policy_hostname* ou *resourcegroup_hostname*. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

5. Na página Recursos, execute as seguintes etapas:
   a. Selecione o tipo de recurso e o Grupo de Disponibilidade do Banco de Dados nas listas suspensas para filtrar a lista de recursos disponíveis.

      Se você adicionou recursos recentemente, eles aparecerão na lista de Recursos Disponíveis somente depois que você atualizar sua lista de recursos.

      Nas seções Recursos Disponíveis e Recursos Selecionados, o nome do banco de dados é exibido com o FQDN do host. Este FQDN indica apenas que o banco de dados está ativo naquele host específico e pode não fazer backup neste host. Você deve selecionar um ou mais servidores de backup na opção Seleção de servidor, onde deseja fazer o backup, caso tenha selecionado a opção **Fazer backup de cópias em servidores a serem selecionados no momento da criação do trabalho de backup** na política.

   b. Digite o nome do recurso na caixa de texto de pesquisa ou role para localizar um recurso.

c. Para mover recursos da seção Recursos Disponíveis para a seção Recursos Selecionados, execute uma das seguintes etapas:

- Selecione **Selecionar automaticamente todos os recursos no mesmo volume de armazenamento** para mover todos os recursos no mesmo volume para a seção Recursos selecionados.
- Selecione os recursos na seção Recursos disponíveis e clique na seta para a direita para movê-los para a seção Recursos selecionados.

  Os grupos de recursos do SnapCenter para Microsoft Exchange Server não podem ter mais de 30 bancos de dados por Snapshot. Se houver mais de 30 bancos de dados em um grupo de recursos, um segundo Snapshot será criado para os bancos de dados adicionais. Portanto, 2 subtarefas são criadas sob a tarefa de backup principal. Para backups com replicação secundária, enquanto a atualização do SnapMirror ou do SnapVault estiver em andamento, pode haver cenários em que a atualização de ambas as subtarefas se sobrepõe. O trabalho de backup principal continua em execução para sempre, mesmo que os logs indiquem que o trabalho foi concluído.

6. Na página Políticas, execute as seguintes etapas:

a. Selecione uma ou mais políticas na lista suspensa.

Você também pode criar uma política clicando em * + *.

Se uma política contiver a opção **Fazer backup de cópias em servidores a serem selecionados no momento da criação do trabalho de backup**, uma opção de seleção de servidor será exibida para selecionar um ou mais servidores. A opção de seleção de servidor listará apenas o servidor onde o banco de dados selecionado está no armazenamento NetApp .

Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

b. Na seção Configurar agendamentos para políticas selecionadas, clique em + *** na coluna *Configurar agendamentos** da política para a qual você deseja configurar o agendamento.

c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento especificando a data de início, a data de expiração e a frequência e clique em **OK**.

Você deve fazer isso para cada frequência listada na política. Os agendamentos configurados são listados na coluna **Agendamentos aplicados** na seção Configurar agendamentos para políticas selecionadas.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

7. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o

comando PowerShell `Set-SmSmtpServer` .

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

8. Revise o resumo e clique em **Concluir**.

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para o Exchange Server

Você deve criar uma conexão de máquina virtual de armazenamento (SVM) e uma credencial antes de usar cmdlets do PowerShell para fazer backup e restaurar.

Antes de começar

- Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.
- Você deve ter as permissões necessárias na função de administrador de infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estejam em andamento.

  As instalações do plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento porque o cache do host pode não ser atualizado e o status dos bancos de dados pode ser exibido na GUI do SnapCenter como “Não disponível para backup” ou "`Não no armazenamento NetApp ".

- Os nomes dos sistemas de armazenamento devem ser exclusivos.

  O SnapCenter não oferece suporte a vários sistemas de armazenamento com o mesmo nome em clusters diferentes. Cada sistema de armazenamento suportado pelo SnapCenter deve ter um nome exclusivo e um endereço IP LIF de dados exclusivo.

Passos

1. Inicie uma sessão de conexão do PowerShell usando o `Open-SmConnection` cmdlet.

   Este exemplo abre uma sessão do PowerShell:

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

2. Crie uma nova conexão com o sistema de armazenamento usando o `Add-SmStorageConnection` cmdlet.

   Este exemplo cria uma nova conexão de sistema de armazenamento:

   ```
   PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Crie uma nova conta Executar como usando o `Add-Credential` cmdlet.

Este exemplo cria uma nova conta Executar como chamada ExchangeAdmin com credenciais do Windows:

```
PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows
-Credential sddev\administrator
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup de bancos de dados do Exchange

Se um banco de dados não fizer parte de nenhum grupo de recursos, você poderá fazer backup do banco de dados ou do Grupo de Disponibilidade do Banco de Dados na página Recursos.

Antes de começar

- Você deve ter criado uma política de backup.
- Você deve ter atribuído o agregado que está sendo usado pela operação de backup ao SVM usado pelo banco de dados.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.
- Se você quiser executar o backup de um banco de dados ou de um grupo de disponibilidade de banco de dados que tenha uma cópia ativa/passiva do banco de dados em um armazenamento NetApp e não NetApp , e tiver selecionado a opção **Fazer backup de cópias ativas** ou **Fazer backup de cópias em servidores a serem selecionados durante o tempo de criação do trabalho de backup** na política, os trabalhos de backup entrarão em estado de aviso. O backup será bem-sucedido para cópias de banco de dados ativas/passivas no armazenamento NetApp e falhará para cópias de banco de dados ativas/passivas em armazenamentos não NetApp .

Melhores práticas: Não execute backups de bancos de dados ativos e passivos ao mesmo tempo. Uma condição de corrida pode ocorrer e um dos backups pode falhar.

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o **plug-in do Microsoft Exchange Server** na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de disponibilidade de banco de dados** na lista **Exibir**.

   Na página Recursos, o  O ícone indica que o banco de dados está em um armazenamento não NetApp .

   > Em um DAG, se uma cópia ativa do banco de dados estiver em um armazenamento não NetApp e pelo menos uma cópia passiva do banco de dados residir em um armazenamento NetApp , você poderá proteger o banco de dados.

   Clique *  * e selecione o nome do host e o tipo de banco de dados para filtrar os recursos. Você pode então clicar em *  * para fechar o painel de filtro.

   - Se você quiser fazer backup de um banco de dados, clique no nome do banco de dados.
     i. Se a visualização Topologia for exibida, clique em **Proteger**.
     ii. Se o assistente Banco de Dados - Proteger Recurso for exibido, continue para a Etapa 3.
   - Se você quiser fazer backup de um Grupo de Disponibilidade de Banco de Dados, clique no nome do Grupo de Disponibilidade de Banco de Dados.
3. Se você quiser especificar um nome de Snapshot personalizado, na página Recursos, marque a caixa de seleção **Usar formato de nome personalizado para cópia de Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

4. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

   > Você também pode criar uma política clicando em *  *.

   > Se uma política contiver a opção **Fazer backup de cópias em servidores a serem selecionados no momento da criação do trabalho de backup**, uma opção de seleção de servidor será exibida para selecionar um ou mais servidores. A opção de seleção de servidor listará apenas o servidor onde o banco de dados selecionado está em um armazenamento NetApp .

   Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique *  * na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

   Onde *policy_name* é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

5. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação de backup realizada no recurso, selecione **Anexar relatório de tarefa**.

   Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

6. Revise o resumo e clique em **Concluir**.

   A página de topologia do banco de dados é exibida.

7. Clique em **Fazer backup agora**.
8. Na página Backup, execute as seguintes etapas:
   a. Se você aplicou várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

      Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

   b. Clique em **Backup**.
9. Monitore o progresso do backup clicando duas vezes no trabalho no painel Atividade na parte inferior da página para exibir a página Detalhes do trabalho.
   - Nas configurações do MetroCluster , o SnapCenter pode não conseguir detectar um relacionamento de proteção após um failover.

     Para mais informações, consulte: "Não é possível detectar o relacionamento SnapMirror ou SnapVault após failover do MetroCluster"

   - Se você estiver fazendo backup de dados do aplicativo em VMDKs e o tamanho do heap Java para o SnapCenter Plug-in for VMware vSphere não for grande o suficiente, o backup poderá falhar.

     Para aumentar o tamanho do heap Java, localize o arquivo de script */opt/netapp/init_scripts/scvservice*. Nesse script, o comando *do_start method* inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: *Java -jar -Xmx8192M -Xms4096M*

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-smconnection  -SMSbaseurl
https://snapctr.demo.netapp.com:8146/
```

O prompt de nome de usuário e senha é exibido.

2. Crie uma política de backup usando o cmdlet Add-SmPolicy.

   Este exemplo cria uma nova política de backup com um backup completo e um backup de log do tipo Exchange:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies
```

   Este exemplo cria uma nova política de backup com um backup completo por hora e um backup de log do tipo Exchange:

```
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'}
```

   Este exemplo cria uma nova política de backup para fazer backup somente de logs do Exchange:

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

3. Descubra recursos do host usando o cmdlet Get-SmResources.

   Este exemplo descobre os recursos para o plug-in do Microsoft Exchange Server no host especificado:

```
C:\PS> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCE
```

4. Adicione um novo grupo de recursos ao SnapCenter usando o cmdlet Add-SmResourceGroup.

   Este exemplo cria um novo grupo de recursos de backup de banco de dados do Exchange Server com a política e os recursos especificados:

```
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_Lo
g_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'}
```

Este exemplo cria um novo grupo de recursos de backup do Grupo de Disponibilidade do Banco de Dados (DAG) do Exchange com a política e os recursos especificados:

```
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_Lo
g_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database
Availability Group";"Names"="DAGSCE0102"}
```

5. Inicie uma nova tarefa de backup usando o cmdlet New-SmBackup.

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

Este exemplo cria um novo backup para armazenamento secundário:

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

6. Visualize o status do trabalho de backup usando o cmdlet Get-SmBackupReport.

Este exemplo exibe um relatório de resumo de todos os trabalhos que foram executados na data especificada:

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

Este exemplo exibe um relatório de resumo de trabalho para um ID de trabalho específico:

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, veja "Guia de referência do cmdlet do

software SnapCenter" .

Fazer backup de grupos de recursos do Exchange

Um grupo de recursos é uma coleção de recursos em um host ou Exchange DAG, e o grupo de recursos pode incluir um DAG inteiro ou bancos de dados individuais. Você pode fazer backup dos grupos de recursos na página Recursos.

Antes de começar

- Você deve ter criado um grupo de recursos com uma política anexada.
- Você deve ter atribuído o agregado que está sendo usado pela operação de backup à máquina virtual de armazenamento (SVM) usada pelo banco de dados.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.
- Se um grupo de recursos tiver vários bancos de dados de hosts diferentes, a operação de backup em alguns dos hosts poderá começar tarde devido a problemas de rede. Você deve configurar o valor de `MaxRetryForUninitializedHosts` em `web.config` usando o `Set-SmConfigSettings` Cmdlet do PowerShell.
- Em um grupo de recursos, se você incluir um Banco de Dados ou Grupo de Disponibilidade de Banco de Dados que tenha uma cópia de banco de dados ativa/passiva em um armazenamento NetApp e não NetApp , e tiver selecionado a opção **Fazer backup de cópias ativas** ou **Fazer backup de cópias em servidores a serem selecionados durante o tempo de criação do trabalho de backup** na política, os trabalhos de backup entrarão em estado de aviso.

  O backup será bem-sucedido para cópias de banco de dados ativas/passivas no armazenamento NetApp e falhará para cópias de banco de dados ativas/passivas em armazenamentos não NetApp .

Sobre esta tarefa

Você pode fazer backup de um grupo de recursos sob demanda na página Recursos. Se um grupo de recursos tiver uma política anexada e um agendamento configurado, os backups ocorrerão automaticamente de acordo com o agendamento.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o **plug-in do Microsoft Exchange Server** na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.

   Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou clicando em * * e, em seguida, selecionando a tag. Você pode então clicar em * * para fechar o painel de filtro.
3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e clique em **Fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
   a. Se você tiver associado várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

b. Clique em **Backup**.

5. Monitore o progresso do backup clicando duas vezes no trabalho no painel Atividade na parte inferior da página para exibir a página Detalhes do trabalho.

Monitorar operações de backup

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Talvez você queira verificar o progresso para determinar quando ele foi concluído ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado correspondente das operações:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **Trabalhos**.
3. Na página Trabalhos, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de backup sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Backup**.
   d. No menu suspenso **Status**, selecione o status do backup.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione uma tarefa de backup e clique em **Detalhes** para visualizar os detalhes da tarefa.

   Embora o status do trabalho de backup seja exibido , ao clicar em detalhes do trabalho, você poderá ver que algumas das tarefas filhas da operação de backup ainda estão em andamento ou marcadas com sinais de alerta.

5. Na página Detalhes do trabalho, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Monitorar operações no painel Atividade

O painel Atividade exibe as cinco operações mais recentes realizadas. O painel Atividade também exibe quando a operação foi iniciada e o status da operação.

O painel Atividade exibe informações sobre operações de backup, restauração, clonagem e backup agendado.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Clique no painel Atividade para visualizar as cinco operações mais recentes.

   Quando você clica em uma das operações, os detalhes da operação são listados na página **Detalhes do trabalho**.

Cancelar operações de backup para banco de dados do Exchange

Você pode cancelar operações de backup que estão na fila.

O que você vai precisar

- Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de backup em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** fica desabilitado para operações que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de backup enfileiradas de outros membros enquanto estiver usando essa função.

Passos

1. Execute uma das seguintes ações:

Do…	Ação
Página do monitor	a. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. b. Selecione a operação e clique em **Cancelar trabalho**.

Do…	Ação
Painel de atividades	a. Após iniciar a operação de backup, clique em * * no painel Atividade para visualizar as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

A operação é cancelada e o recurso é revertido ao estado anterior.

Exibir backups do Exchange na página Topologia

Ao se preparar para fazer backup de um recurso, pode ser útil visualizar uma representação gráfica de todos os backups nos armazenamentos primário e secundário.

Sobre esta tarefa

Na página Topologia, você pode ver todos os backups disponíveis para o recurso ou grupo de recursos selecionado. Você pode visualizar os detalhes desses backups e selecioná-los para executar operações de proteção de dados.

Você pode revisar o ícone a seguir na exibição Gerenciar cópias para determinar se os backups estão disponíveis no armazenamento primário ou secundário (cópias espelhadas ou cópias do Vault).

-  exibe o número de backups disponíveis no armazenamento primário.
-  exibe o número de backups que são espelhados no armazenamento secundário usando a tecnologia SnapMirror .
-  exibe o número de backups que são replicados no armazenamento secundário usando a tecnologia SnapVault .
  - O número de backups exibidos inclui os backups excluídos do armazenamento secundário.

    Por exemplo, se você criou 6 backups usando uma política para manter apenas 4 backups, o número de backups exibidos será 6.

Melhores práticas: para garantir que o número correto de backups replicados seja exibido, recomendamos que você atualize a topologia.

Se você tiver um relacionamento secundário como sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC]), poderá ver os seguintes ícones adicionais:

-  O site de réplica está no ar.

-  O site de réplicas está fora do ar.
-  O espelho secundário ou o relacionamento do cofre não foram restabelecidos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o banco de dados, o recurso ou o grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso na exibição de detalhes do banco de dados ou na exibição de detalhes do grupo de recursos.

   Se o recurso estiver protegido, a página Topologia do recurso selecionado será exibida.

4. Revise a seção do cartão Resumo para ver um resumo do número de backups disponíveis no armazenamento primário e secundário.

   A seção Cartão de Resumo exibe o número total de backups e o número total de backups de log.

   Clicar no botão **Atualizar** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clicar no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Uma programação semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo estiver distribuído em vários volumes, o tempo de expiração do SnapLock para o backup será o maior tempo de expiração do SnapLock definido para um Snapshot em um volume. O maior tempo de expiração do SnapLock é recuperado do ONTAP.

   Para sincronização ativa do SnapMirror , clicar no botão **Atualizar** atualiza o inventário de backup do SnapCenter consultando o ONTAP para sites primários e de réplica. Uma programação semanal também executa essa atividade para todos os bancos de dados que contêm o relacionamento de sincronização ativo do SnapMirror .

   - Para sincronização ativa do SnapMirror e somente para o ONTAP 9.14.1, os relacionamentos Async Mirror ou Async MirrorVault com o novo destino primário devem ser configurados manualmente após o failover. A partir do ONTAP 9.15.1, o Async Mirror ou o Async MirrorVault são configurados automaticamente para o novo destino primário após o failover.
   - Após o failover, um backup deve ser criado para que o SnapCenter esteja ciente do failover. Você pode clicar em **Atualizar** somente após um backup ter sido criado.
5. Na exibição Gerenciar cópias, clique em **Backups** do armazenamento primário ou secundário para ver detalhes de um backup.

   Os detalhes dos backups são exibidos em formato de tabela.

6. Selecione o backup na tabela e clique nos ícones de proteção de dados para executar operações de restauração, renomeação e exclusão.

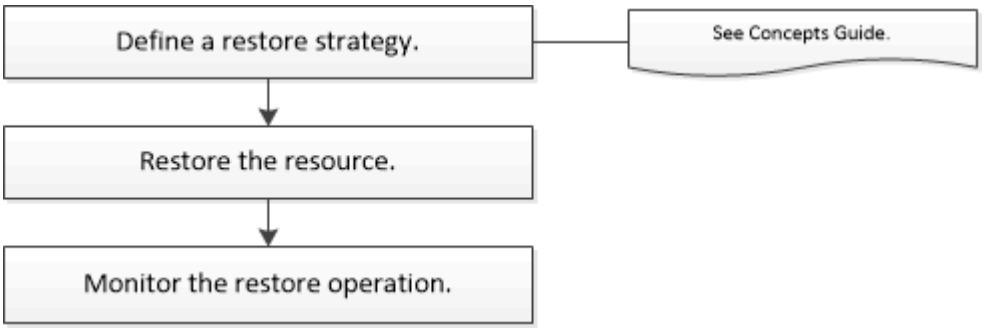
   Não é possível renomear ou excluir backups que estejam no armazenamento secundário. A exclusão de Snapshots é controlada pelas configurações de retenção do ONTAP .

Restaurar recursos do Exchange

Fluxo de trabalho de restauração

Você pode usar o SnapCenter para restaurar bancos de dados do Exchange restaurando um ou mais backups para seu sistema de arquivos ativo.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar as operações de restauração do banco de dados do Exchange:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup e restauração. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte "Guia de referência do cmdlet do software SnapCenter" .

Requisitos para restaurar um banco de dados do Exchange

Antes de restaurar um banco de dados do Exchange Server a partir de um backup do SnapCenter Plug-in para Microsoft Exchange Server, você deve garantir que vários requisitos sejam atendidos.

Para usar a funcionalidade de restauração completamente, você deve atualizar o SnapCenter Server e o SnapCenter Plug-in para o banco de dados do Exchange para 4.6.

- O Exchange Server deve estar online e em execução antes que você possa restaurar um banco de dados.
- Os bancos de dados devem existir no Exchange Server.

  Não há suporte para restauração de bancos de dados excluídos.

- Os agendamentos do SnapCenter para o banco de dados devem ser suspensos.
- O SnapCenter Server e o host do SnapCenter Plug-in para Microsoft Exchange Server devem estar conectados ao armazenamento primário e secundário que contém os backups que você deseja restaurar.

Restaurar bancos de dados do Exchange

Você pode usar o SnapCenter para restaurar bancos de dados do Exchange com backup.

Antes de começar

- Você deve ter feito backup dos grupos de recursos, do banco de dados ou dos Grupos de Disponibilidade

de Banco de Dados (DAGs).

- Quando o banco de dados do Exchange é migrado para outro local, a operação de restauração não funciona para backups antigos.
- Se você estiver replicando Snapshots para um espelho ou cofre, o administrador do SnapCenter deverá ter atribuído a você as SVMs para os volumes de origem e de destino.
- Em um DAG, se uma cópia ativa do banco de dados estiver em um armazenamento não NetApp e você quiser restaurar a partir do backup da cópia passiva do banco de dados que está em um armazenamento NetApp , torne a cópia passiva (armazenamento NetApp) como cópia ativa, atualize os recursos e execute a operação de restauração.

  Execute o `Move-ActiveMailboxDatabase` comando para fazer a cópia passiva do banco de dados como cópia ativa do banco de dados.

  O "Documentação da Microsoft" contém informações sobre este comando.

Sobre esta tarefa

- Quando a operação de restauração é executada em um banco de dados, o banco de dados é montado novamente no mesmo host e nenhum novo volume é criado.
- Os backups em nível de DAG devem ser restaurados de bancos de dados individuais.
- A restauração completa do disco não é suportada quando existem arquivos diferentes do banco de dados do Exchange (.edb).

  O plug-in para Exchange não executa uma restauração completa em um disco se o disco contiver arquivos do Exchange, como aqueles usados para replicação. Quando uma restauração completa pode afetar a funcionalidade do Exchange, o Plug-in for Exchange executa uma única operação de restauração de arquivo.

- O plug-in para Exchange não pode restaurar unidades criptografadas pelo BitLocker.
- O SCRIPTS_PATH é definido usando a chave PredefinedWindowsScriptsDirectory localizada no arquivo SMCoreServiceHost.exe.Config do host do plug-in.

  Se necessário, você pode alterar esse caminho e reiniciar o serviço SMcore. É recomendável que você use o caminho padrão por segurança.

  O valor da chave pode ser exibido no swagger por meio da API: API /4.7/configsettings

  Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .
- Para a operação de restauração de sincronização ativa do SnapMirror , você deve selecionar o backup do local principal.

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** no canto superior esquerdo da página Recursos.
2. Selecione o plug-in do Exchange Server na lista suspensa.
3. Na página Recursos, selecione **Banco de dados** na lista Exibir.
4. Selecione o banco de dados na lista.
5. Na exibição Gerenciar cópias, selecione **Backups**, na tabela Backups primários e clique em *  *.
6. Na página Opções, selecione uma das seguintes opções de backup de log:

Opção	Descrição
Todos os backups de log	Selecione **Todos os backups de log** para executar uma operação de restauração de backup atualizada para restaurar todos os backups de log disponíveis após o backup completo.
Por backups de log até	Escolha **Por backups de log até** para executar uma operação de restauração pontual, que restaura o banco de dados com base em backups de log até o log selecionado. O número de logs exibidos na lista suspensa é baseado em UTM. Por exemplo, se a retenção de backup completo for 5 e a retenção UTM for 3, o número de backups de log disponíveis será 5, mas no menu suspenso apenas 3 logs serão listados para executar a operação de restauração.
Por data específica até	Escolha **Por data específica até** para especificar a data e a hora até as quais os logs de transações serão aplicados ao banco de dados restaurado. Esta operação de restauração pontual restaura entradas de log de transações que foram registradas até o último backup na data e hora especificadas.
Nenhum	Escolha **Nenhum** quando precisar restaurar apenas o backup completo, sem nenhum backup de log.

Você pode executar uma das seguintes ações:

- **Recuperar e montar banco de dados após a restauração** - Esta opção é selecionada por padrão.
- **Não verifique a integridade dos logs de transações no backup antes da restauração** - Por padrão, o SnapCenter verifica a integridade dos logs de transações em um backup antes de executar uma operação de restauração.

  Melhores práticas: Você não deve selecionar esta opção.

7. Na página Script, insira o caminho e os argumentos do prescript ou postscript que devem ser executados antes ou depois da operação de restauração, respectivamente.

   Os argumentos de prescrição de restauração incluem $Database e $ServerInstance.

   Os argumentos de restauração do postscript incluem $Database, $ServerInstance, $BackupName, $LogDirectory e $TargetServerInstance.

   Você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.

   O caminho de prescrições ou pós-escritos não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPTS_PATH.

8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail.

9. Revise o resumo e clique em **Concluir**.
10. Você pode visualizar o status do trabalho de restauração expandindo o painel Atividade na parte inferior da página.

    Você deve monitorar o processo de restauração usando a página **Monitor** > **Tarefas**.

Ao restaurar um banco de dados ativo a partir de um backup, o banco de dados passivo pode entrar em estado suspenso ou com falha se houver um atraso entre a réplica e o banco de dados ativo.

A mudança de estado pode ocorrer quando a cadeia de logs do banco de dados ativo se bifurca e inicia uma nova ramificação, o que interrompe a replicação. O Exchange Server tenta corrigir a réplica, mas se não conseguir, após a restauração, você deve criar um novo backup e, em seguida, propagar novamente a réplica.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o `Open-SmConnection` cmdlet.

```
Open-smconnection  -SMSbaseurl
https://snapctr.demo.netapp.com:8146/
```

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando o `Get-SmBackup` cmdlet.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
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. Restaurar dados do backup usando o `Restore-SmBackup` cmdlet.

   Este exemplo restaura um backup atualizado:

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
-IsRecoverMount:$true
```

   Este exemplo restaura um backup de um ponto no tempo:

```
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
```

   Este exemplo restaura um backup no armazenamento secundário para o histórico primário:

```
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
```

   O `-archive` O parâmetro permite que você especifique os volumes primário e secundário que deseja usar para a restauração.

O `-IsRecoverMount:$true` parâmetro permite que você monte o banco de dados após a restauração.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Recuperação granular de e-mails e caixas de correio

O software Single Mailbox Recovery (SMBR) permite que você restaure e recupere e-mails ou caixas de correio em vez do banco de dados completo do Exchange.

Restaurar um banco de dados completo apenas para recuperar um único e-mail consumirá muito tempo e recursos. O SMBR ajuda a recuperar rapidamente os e-mails criando uma cópia clone do Snapshot e, em seguida, usando APIs da Microsoft para montar a caixa de correio no SMBR. Para obter informações sobre como usar o SMBR, consulte "Guia de Administração do SMBR" .

Para obter informações adicionais sobre SMBR, consulte o seguinte:

- "Como restaurar manualmente um único item com SMBR (também aplicável para restaurações do Ontrack Power Control)"
- "Como restaurar do armazenamento secundário no SMBR com o SnapCenter"
- "Recuperando e-mails do Microsoft Exchange do SnapVault usando SMBR"

Restaurar um banco de dados do Exchange Server a partir do armazenamento secundário

Você pode restaurar um banco de dados do Exchange Server com backup a partir de um armazenamento secundário (espelho ou cofre).

Você deve ter replicado os Snapshots do armazenamento primário para um armazenamento secundário.

Sobre esta tarefa

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .
- Para a operação de restauração de sincronização ativa do SnapMirror , você deve selecionar o backup do local principal.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione **Plug-in do Microsoft Exchange Server** na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista suspensa **Exibir**.
3. Selecione o banco de dados ou o grupo de recursos.

   A página de topologia do banco de dados ou do grupo de recursos é exibida.

4. Na seção Gerenciar cópias, selecione **Backups** do sistema de armazenamento secundário (espelho ou cofre).

5. Selecione o backup na lista e clique em  .
6. Na página Local, escolha o volume de destino para restaurar o recurso selecionado.
7. Conclua o assistente de restauração, revise o resumo e clique em **Concluir**.

Reproduzir uma réplica de nó passivo do Exchange

Se você precisar repropagar uma cópia de réplica, por exemplo, quando uma cópia estiver corrompida, você poderá repropagar para o backup mais recente usando o recurso de repropagação no SnapCenter.

Antes de começar

Você deve ter criado um backup do banco de dados que deseja propagar novamente.

+ Para evitar atrasos entre os nós, você pode criar um novo backup antes de executar uma operação de nova propagação ou escolher o host com o backup mais recente.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione **Plug-in do Microsoft Exchange Server** na lista.
2. Na página Recursos, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para replantar um único banco de dados	Selecione **Banco de dados** na lista Exibir.
Para replantar bancos de dados em um DAG	Selecione **Grupo de Disponibilidade de Banco de Dados** na lista Exibir.

3. Selecione o recurso que você deseja propagar novamente.
4. Na página Gerenciar cópias, clique em **Repropagar**.
5. Na lista de cópias de bancos de dados não íntegros no assistente Reseed, selecione aquela que você deseja reseed e clique em **Avançar**.
6. Na janela Host, selecione o host com o backup do qual você deseja repropagar e clique em **Avançar**.
7. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail.

8. Revise o resumo e clique em **Concluir**.
9. Você pode visualizar o status do trabalho expandindo o painel Atividade na parte inferior da página.

A operação de nova propagação não será suportada se a cópia passiva do banco de dados residir em um armazenamento que não seja da NetApp .

Repropagar uma réplica usando cmdlets do PowerShell para banco de dados do Exchange

Você pode usar cmdlets do PowerShell para restaurar uma réplica não íntegra usando a cópia mais recente no mesmo host ou a cópia mais recente de um host alternativo.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o `Open-SmConnection` cmdlet.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Resemelhe o banco de dados usando o `reseed-SmDagReplicaCopy` cmdlet.

   Este exemplo repete a cópia com falha do banco de dados chamado execdb no host "mva-rx200.netapp.com" usando o backup mais recente naquele host.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb
```

   Este exemplo ressemeia a cópia com falha do banco de dados chamado execdb usando o backup mais recente do banco de dados (produção/cópia) em um host alternativo "mva-rx201.netapp.com".

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb -BackupHost "mva-rx201.netapp.com"
```

Monitorar operações de restauração

Você pode monitorar o progresso de diferentes operações de restauração do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa tomar.

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso

- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de restauração sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Restaurar**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Aplicar** para visualizar as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Cancelar operações de restauração para banco de dados do Exchange

Você pode cancelar trabalhos de restauração que estão na fila.

Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações de restauração.

Sobre esta tarefa

- Você pode cancelar uma operação de restauração enfileirada na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de restauração em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de restauração enfileiradas.
- O botão **Cancelar tarefa** fica desabilitado para operações de restauração que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de restauração enfileiradas de outros membros enquanto estiver usando essa função.

Etapa

Execute uma das seguintes ações:

Do…	Ação
Página do monitor	1. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. 2. Selecione o trabalho e clique em **Cancelar trabalho**.
Painel de atividades	1. Após iniciar a operação de restauração, clique em  no painel Atividade para visualizar as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

Proteja o IBM Db2

Plug-in SnapCenter para IBM Db2

Visão geral do plug-in SnapCenter para IBM Db2

O SnapCenter Plug-in para IBM Db2 Database é um componente do lado do host do SnapCenter software NetApp SnapCenter que permite o gerenciamento de proteção de dados com reconhecimento de aplicativo de bancos de dados IBM Db2. O plug-in para IBM Db2 Database automatiza o backup, a restauração e a clonagem de bancos de dados IBM Db2 no seu ambiente SnapCenter .

- O SnapCenter 6.0 é compatível com o IBM Db2 10.5 e versões posteriores.
- O SnapCenter 6.0.1 é compatível com IBM Db2 9.7.x e posteriores. Além disso, a partir do SnapCenter 6.0.1, o IBM Db2 no AIX é suportado.

O SnapCenter oferece suporte a configurações de instância única e múltiplas instâncias do Db2. Você pode usar o Plug-in para IBM Db2 Database em ambientes Linux e Windows. Em ambientes Windows, o Db2 será suportado como recurso manual.

O ambiente Db2 pureScale e os sistemas Db2 multi-nó (DPF) não são suportados.

Quando o plug-in para o IBM Db2 Database estiver instalado, você poderá usar o SnapCenter com a tecnologia NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume. Você também pode usar o plug-in com a tecnologia NetApp SnapVault para executar a replicação de backup de disco para disco para conformidade com os padrões.

O plug-in SnapCenter para Db2 oferece suporte a NFS e SAN em layouts de armazenamento de arquivos ONTAP e Azure NetApp .

O layout de armazenamento virtual VMDK, vVol e RDM é suportado.

O que você pode fazer usando o plug-in SnapCenter para IBM Db2

Ao instalar o Plug-in para IBM Db2 Database em seu ambiente, você pode usar o SnapCenter para fazer backup, restaurar e clonar bancos de dados IBM Db2 e seus recursos. Você também pode executar tarefas de suporte a essas operações.

- Adicionar bancos de dados.
- Crie backups.
- Restaurar a partir de backups.
- Clonar backups.
- Agende operações de backup.
- Monitore operações de backup, restauração e clonagem.
- Visualize relatórios de operações de backup, restauração e clonagem.

Recursos do plug-in SnapCenter para IBM Db2

O SnapCenter integra-se ao aplicativo plug-in e às tecnologias NetApp no sistema de armazenamento. Para trabalhar com o Plug-in para IBM Db2 Database, use a interface gráfica do usuário do SnapCenter .

- **Interface gráfica de usuário unificada**

  A interface do SnapCenter fornece padronização e consistência entre plug-ins e ambientes. A interface do SnapCenter permite que você conclua operações consistentes de backup, restauração e clonagem em plug-ins, use relatórios centralizados, use visualizações de painel rápidas, configure o controle de acesso baseado em função (RBAC) e monitore trabalhos em todos os plug-ins.

- **Administração central automatizada**

  Você pode agendar operações de backup, configurar retenção de backup baseada em políticas e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- *Tecnologia de cópia instantânea não disruptiva da NetApp *

  O SnapCenter usa a tecnologia de snapshot da NetApp com o Plug-in para IBM Db2 Database para fazer backup de recursos.

O uso do plug-in para IBM Db2 também oferece os seguintes benefícios:

- Suporte para fluxos de trabalho de backup, restauração e clonagem
- Segurança com suporte RBAC e delegação centralizada de funções

  Você também pode definir as credenciais para que os usuários autorizados do SnapCenter tenham permissões no nível do aplicativo.

- Criação de cópias de recursos com eficiência de espaço e em um determinado momento para testes ou extração de dados usando a tecnologia NetApp FlexClone

  Uma licença FlexClone é necessária no sistema de armazenamento onde você deseja criar o clone.

- Suporte para o recurso de instantâneo do grupo de consistência (CG) do ONTAP como parte da criação de backups.
- Capacidade de executar vários backups simultaneamente em vários hosts de recursos

  Em uma única operação, os snapshots são consolidados quando recursos em um único host compartilham o mesmo volume.

- Capacidade de criar snapshots usando comandos externos.
- Suporte para Linux LVM no sistema de arquivos XFS.

Tipos de armazenamento suportados pelo SnapCenter Plug-in para IBM Db2

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e virtuais (VMs). Você deve verificar o suporte para seu tipo de armazenamento antes de instalar o SnapCenter Plug-in para IBM Db2.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados por FC • LUNs conectados por iSCSI • Volumes conectados ao NFS
VMware ESXi	• LUNs RDM conectados por um FC ou iSCSI ESXi HBAA varredura de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluída porque o SnapCenter verifica todos os adaptadores de barramento de host presentes no host. Você pode editar o arquivo **LinuxConfig.pm** localizado em */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* para definir o valor do parâmetro **SCSI_HOSTS_OPTIMIZED_RESCAN** como 1 para verificar novamente apenas os HBAs listados em HBA_DRIVER_NAMES. • LUNs iSCSI conectados diretamente ao sistema convidado pelo iniciador iSCSI • VMDKs em armazenamentos de dados NFS • VMDKs em VMFS criados • Volumes NFS conectados diretamente ao sistema convidado • Armazenamentos de dados vVol em NFS e SAN O armazenamento de dados vVol só pode ser provisionado com o ONTAP Tools para VMware vSphere.

Privilégios ONTAP mínimos necessários para o plug-in IBM Db2

Os privilégios mínimos do ONTAP necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos de acesso total: privilégios mínimos necessários para ONTAP 9.12.1 e posterior
  - evento generate-autosupport-log
  - histórico de trabalho mostrar
  - parada de trabalho
  - lua
  - lun criar
  - lun criar
  - lun criar

- lun delete
- lun igroup adicionar
- lun igroup criar
- lun igroup excluir
- renomear lun igroup
- renomear lun igroup
- show do lun igroup
- mapeamento lun add-reporting-nodes
- criação de mapeamento lun
- exclusão de mapeamento lun
- mapeamento lun remove-reporting-nodes
- show de mapeamento lunar
- lun modificar
- volume de entrada lun
- lua offline
- lua online
- lun persistente-reserva clara
- redimensionamento de lun
- série lun
- show de lua
- política de adição de regra do snapmirror
- regra de modificação de política do snapmirror
- política de remoção do snapmirror
- política do snapmirror mostrar
- restauração do snapmirror
- show de espelhos instantâneos
- histórico de exibição do snapmirror
- atualização do snapmirror
- atualização do snapmirror-ls-set
- lista-destinos do snapmirror
- versão
- criação de clone de volume
- show de clones de volume
- volume clone split start
- volume clone divisão parada
- volume criar
- destruição de volume

    - clone de arquivo de volume criar
    - arquivo de volume mostrar-uso-do-disco
    - volume offline
    - volume on-line
    - modificação de volume
    - volume qtree criar
    - volume qtree delete
    - volume qtree modificar
    - volume qtree mostrar
    - restrição de volume
    - show de volume
    - criação de instantâneo de volume
    - exclusão de instantâneo de volume
    - modificação de instantâneo de volume
    - instantâneo de volume modificar-tempo-de-expiração-do-snaplock
    - renomeação de instantâneo de volume
    - restauração de instantâneo de volume
    - arquivo de restauração de instantâneo de volume
    - exibição de instantâneo de volume
    - desmontagem de volume
    - cifs do vserver
    - vserver cifs compartilhar criar
    - vserver cifs compartilhar excluir
    - vserver cifs shadowcopy mostrar
    - vserver cifs compartilhar mostrar
    - vserver cifs mostrar
    - política de exportação do vserver
    - criação de política de exportação do vserver
    - exclusão da política de exportação do vserver
    - criação de regra de política de exportação do vserver
    - mostrar regra de política de exportação do vserver
    - mostrar política de exportação do vserver
    - vserver iscsi
    - mostrar conexão iscsi do vserver
    - vserver mostrar
- Comandos somente leitura: privilégios mínimos necessários para ONTAP 8.3.0 e posterior
    - interface de rede

- exibição de interface de rede
- vserver

Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para IBM Db2

Você pode usar um plug-in SnapCenter com a tecnologia ONTAP SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia ONTAP SnapVault para executar replicação de backup de disco para disco para conformidade com padrões e outros propósitos relacionados à governança. Antes de executar essas tarefas, você deve configurar um relacionamento de proteção de dados entre os volumes de origem e destino e inicializar o relacionamento.

O SnapCenter executa as atualizações no SnapMirror e no SnapVault após concluir a operação Snapshot. As atualizações do SnapMirror e do SnapVault são executadas como parte do trabalho do SnapCenter ; não crie uma programação ONTAP separada.

Se você estiver acessando o SnapCenter a partir de um produto NetApp SnapManager e estiver satisfeito com os relacionamentos de proteção de dados configurados, pode pular esta seção.

Um relacionamento de proteção de dados replica dados do armazenamento primário (o volume de origem) para o armazenamento secundário (o volume de destino). Quando você inicializa o relacionamento, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não oferece suporte a relacionamentos em cascata entre volumes SnapMirror e SnapVault (**Primário** > **Espelho** > **Cofre**). Você deve usar relacionamentos fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis em termos de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis em termos de versão e como configurá-los, consulte "Documentação do ONTAP" .

Estratégia de backup para IBM Db2

Definir uma estratégia de backup para IBM Db2

Definir uma estratégia de backup antes de criar suas tarefas de backup ajuda você a ter os backups necessários para restaurar ou clonar seus recursos com sucesso. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (RTO) e objetivo de ponto de recuperação (RPO) determinam em grande parte sua estratégia de backup.

Sobre esta tarefa

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. RTO é o tempo em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. SLA, RTO e RPO contribuem para a estratégia de proteção de dados.

Passos

1. Determine quando você deve fazer backup dos seus recursos.
2. Decida quantos trabalhos de backup você precisa.
3. Decida como nomear seus backups.
4. Decida se você deseja criar uma política baseada em cópia de instantâneo para fazer backup de instantâneos consistentes com o aplicativo do banco de dados.
5. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção de longo prazo.
6. Determine o período de retenção dos snapshots no sistema de armazenamento de origem e no destino do SnapMirror .
7. Determine se você deseja executar algum comando antes ou depois da operação de backup e forneça uma prescrição ou pós-escrito.

Descoberta automática de recursos no host Linux

Os recursos são bancos de dados e instâncias do IBM Db2 no host Linux que são gerenciados pelo SnapCenter. Após instalar o plug-in SnapCenter para IBM Db2, os bancos de dados IBM Db2 de todas as instâncias naquele host Linux são descobertos automaticamente e exibidos na página Recursos.

Tipo de backups suportados

O tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter oferece suporte ao tipo de backup baseado em cópia de snapshot para bancos de dados IBM Db2.

Backup baseado em cópia instantânea

Os backups baseados em cópias de instantâneo aproveitam a tecnologia de instantâneo da NetApp para criar cópias on-line somente leitura dos volumes nos quais os bancos de dados IBM Db2 residem.

Como o plug-in SnapCenter para IBM Db2 usa instantâneos de grupo de consistência

Você pode usar o plug-in para criar instantâneos de grupos de consistência para grupos de recursos. Um grupo de consistência é um contêiner que pode abrigar vários volumes para que você possa gerenciá-los como uma única entidade. Um grupo de consistência é composto por instantâneos simultâneos de vários volumes, fornecendo cópias consistentes de um grupo de volumes.

Você também pode especificar o tempo de espera para que o controlador de armazenamento agrupe snapshots de forma consistente. As opções de tempo de espera disponíveis são **Urgente**, **Médio** e **Relaxado**. Você também pode habilitar ou desabilitar a sincronização do Write Anywhere File Layout (WAFL) durante a operação consistente de snapshot de grupo. A sincronização do WAFL melhora o desempenho de um instantâneo de grupo de consistência.

Como o SnapCenter gerencia a manutenção de backups de dados

O SnapCenter gerencia a manutenção de backups de dados nos níveis do sistema de armazenamento e do sistema de arquivos.

Os snapshots no armazenamento primário ou secundário e suas entradas correspondentes no catálogo do IBM Db2 são excluídos com base nas configurações de retenção.

Considerações para determinar agendamentos de backup para IBM Db2

O fator mais crítico na determinação de um cronograma de backup é a taxa de alteração do recurso. Você pode fazer backup de um recurso muito utilizado a cada hora, enquanto pode fazer backup de um recurso raramente utilizado uma vez por dia. Outros fatores incluem a importância do recurso para sua organização, seu acordo de nível de serviço (SLA) e seu objetivo de ponto de recuperação (RPO).

Os agendamentos de backup têm duas partes, conforme a seguir:

- Frequência de backup (com que frequência os backups devem ser realizados)

  A frequência de backup, também chamada de tipo de agendamento para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como horária, diária, semanal ou mensal.

- Agendamentos de backup (exatamente quando os backups devem ser executados)

  Os agendamentos de backup fazem parte de uma configuração de recurso ou grupo de recursos. Por exemplo, se você tiver um grupo de recursos com uma política configurada para backups semanais, poderá configurar o agendamento para fazer backup todas as quintas-feiras às 22h.

Número de tarefas de backup necessárias para o IBM Db2

Os fatores que determinam o número de tarefas de backup necessárias incluem o tamanho do recurso, o número de volumes usados, a taxa de alteração do recurso e seu Contrato de Nível de Serviço (SLA).

Convenções de nomenclatura de backup para plug-in para bancos de dados IBM Db2

Você pode usar a convenção de nomenclatura padrão do Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um registro de data e hora aos nomes de instantâneos que ajuda a identificar quando as cópias foram criadas.

O Snapshot usa a seguinte convenção de nomenclatura padrão:

```
resourcegroupname_hostname_timestamp
```

Você deve nomear seus grupos de recursos de backup logicamente, como no exemplo a seguir:

```
dts1_mach1x88_03-12-2015_23.17.26
```

Neste exemplo, os elementos de sintaxe têm os seguintes significados:

- *dts1* é o nome do grupo de recursos.

- *mach1x88* é o nome do host.
- *03-12-2015_23.17.26* é a data e o registro de data e hora.

Como alternativa, você pode especificar o formato do nome do Snapshot ao proteger recursos ou grupos de recursos selecionando **Usar formato de nome personalizado para cópia do Snapshot**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do registro de data e hora é adicionado ao nome do Snapshot.

Estratégia de restauração e recuperação para IBM Db2

Definir uma estratégia de restauração e recuperação para recursos do IBM Db2

Você deve definir uma estratégia antes de restaurar e recuperar seu banco de dados para que possa executar operações de restauração e recuperação com sucesso.

Somente a recuperação manual do banco de dados é suportada.

Passos

1. Determinar as estratégias de restauração suportadas para recursos IBM Db2 adicionados manualmente
2. Determinar as estratégias de restauração suportadas para bancos de dados IBM Db2 descobertos automaticamente

Tipos de estratégias de restauração suportadas para recursos IBM Db2 adicionados manualmente

Você deve definir uma estratégia antes de poder executar com sucesso operações de restauração usando o SnapCenter. Há dois tipos de estratégias de restauração para recursos do IBM Db2 adicionados manualmente.

Não é possível recuperar recursos do IBM Db2 adicionados manualmente.

Restauração completa de recursos

- Restaura todos os volumes, qtrees e LUNs de um recurso

Se o recurso contiver volumes ou qtrees, os instantâneos tirados após o instantâneo selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

Tipo de estratégia de restauração com suporte para IBM Db2 descoberto automaticamente

Você deve definir uma estratégia antes de poder executar com sucesso operações de restauração usando o SnapCenter.

A restauração completa de recursos é a estratégia de restauração suportada por bancos de dados IBM Db2 descobertos automaticamente. Isso restaura todos os volumes, qtrees e LUNs de um recurso.

Tipos de operações de restauração para IBM Db2 descoberto automaticamente

O plug-in SnapCenter para IBM Db2 oferece suporte a Single File SnapRestore e tipos de restauração de conexão e cópia para bancos de dados IBM Db2 descobertos automaticamente.

O Single File SnapRestore é executado em ambientes NFS para os seguintes cenários:

- Se apenas a opção **Recurso Completo** for selecionada
- Quando o backup selecionado for de um local secundário do SnapMirror ou SnapVault e a opção **Recurso Completo** for selecionada

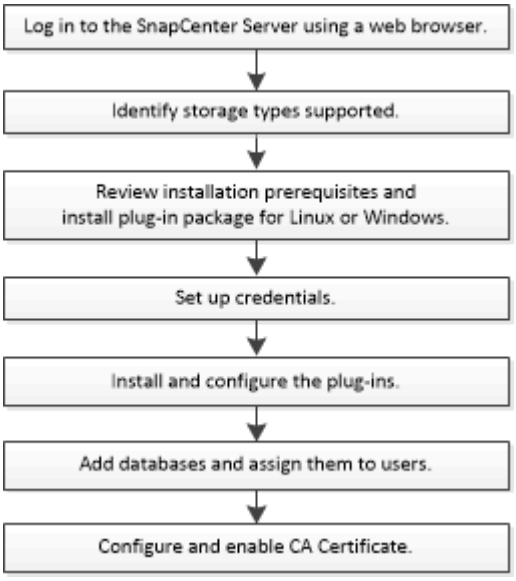
O Single File SnapRestore é executado em ambientes SAN para os seguintes cenários:

- Se apenas a opção **Recurso Completo** for selecionada
- Quando o backup é selecionado de um local secundário do SnapMirror ou SnapVault e a opção **Recurso Completo** é selecionada

Prepare-se para instalar o plug-in SnapCenter para IBM Db2

Fluxo de trabalho de instalação do plug-in SnapCenter para IBM Db2

Você deve instalar e configurar o SnapCenter Plug-in para IBM Db2 se quiser proteger bancos de dados IBM Db2.



Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Windows, Linux ou AIX

Antes de adicionar um host e instalar os pacotes de plug-in, você deve concluir todos os requisitos. Plug-in SnapCenter para IBM Db2 compatível com ambientes Windows, Linux e AIX.

- Você deve ter instalado o Java 11 no seu host.

O IBM Java não é suportado em hosts Windows e Linux.

- No Windows, o Plug-in Creator Service deve ser executado usando o usuário do Windows “LocalSystem”, que é o comportamento padrão quando o Plug-in para IBM Db2 é instalado como administrador de domínio.
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host. O plug-in SnapCenter para Microsoft Windows será implantado por padrão com o plug-in IBM Db2 em hosts Windows.
- O SnapCenter Server deve ter acesso à porta 8145 ou personalizada do plug-in para host IBM Db2.

Hosts do Windows

- Você deve ter um usuário de domínio com privilégios de administrador local e permissões de login local no host remoto.
- Ao instalar o Plug-in para IBM Db2 em um host Windows, o SnapCenter Plug-in para Microsoft Windows é instalado automaticamente.
- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 no seu host Windows.

  "Baixe JAVA para Windows"

  "Ferramenta de Matriz de Interoperabilidade da NetApp"

Hosts Linux e AIX

- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 no seu host Linux.

  "Baixe JAVA para Linux"

  "Baixe JAVA para AIX"

  "Ferramenta de Matriz de Interoperabilidade da NetApp"

- Para bancos de dados IBM Db2 em execução em um host Linux, ao instalar o Plug-in para IBM Db2, o SnapCenter Plug-in para UNIX é instalado automaticamente.
- Você deve ter **bash** como o shell padrão para instalação de plug-ins.

Comandos suplementares

Para executar um comando suplementar no SnapCenter Plug-in para IBM Db2, você deve incluí-lo no arquivo *allowed_commands.config*.

- Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Para permitir comandos suplementares no host do plug-in, abra o arquivo *allowed_commands.config* em um editor. Digite cada comando em uma linha separada e os comandos não diferenciam maiúsculas de

minúsculas. Certifique-se de especificar o caminho totalmente qualificado e coloque-o entre aspas (") se ele contiver espaços.

Por exemplo:

comando: montar

comando: umount

comando: "C:\Arquivos de Programas\ NetApp\Comandos do SnapCreator\sdcli.exe"

comando: myscript.bat

Se o arquivo *allowed_commands.config* não estiver presente, os comandos ou a execução do script serão bloqueados e o fluxo de trabalho falhará com o seguinte erro:

"[/mnt/mount -a] execução não permitida. Autorize adicionando o comando no arquivo %s no host do plugin."

Se o comando ou script não estiver presente no *allowed_commands.config*, a execução do comando ou script será bloqueada e o fluxo de trabalho falhará com o seguinte erro:

"[/mnt/mount -a] execução não permitida. Autorize adicionando o comando no arquivo %s no host do plugin."

Você não deve usar uma entrada curinga (*) para permitir todos os comandos.

Configurar privilégios sudo para usuários não root para host Linux

O SnapCenter permite que um usuário não root instale o pacote de plug-ins do SnapCenter para Linux e inicie o processo de plug-in. Os processos do plug-in serão executados como um usuário não root efetivo. Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se a umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro dela tenham permissão de 555. Caso contrário, a instalação do plug-in poderá falhar.
- Para o usuário não root, certifique-se de que o nome do usuário não root e o nome do grupo do usuário sejam os mesmos.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos do código de autenticação de mensagens: MACs hmac-sha2-256 e MACs hmac-sha2-512.

  Reinicie o serviço sshd após atualizar o arquivo de configuração.

  Exemplo:

```
#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
```

Sobre esta tarefa

Você deve configurar privilégios sudo para que o usuário não root forneça acesso aos seguintes caminhos:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /localização_personalizada/ NetApp/snapcenter/spl/instalação/plugins/desinstalação
- /localização_personalizada/ NetApp/snapcenter/spl/bin/spl

Passos

1. Efetue login no host Linux no qual você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
2. Adicione as seguintes linhas ao arquivo /etc/sudoers usando o utilitário visudo Linux.

```
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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Se você tiver uma configuração RAC, junto com os outros comandos permitidos, você deve adicionar o seguinte ao arquivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Você pode obter o valor de *crs_home* do arquivo */etc/oracle/olr.loc*.

LINUX_USER é o nome do usuário não root que você criou.

Você pode obter o *checksum_value* do arquivo **sc_unix_plugins_checksum.txt**, localizado em:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Linux.

O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Configurar privilégios sudo para usuários não root para host AIX

O SnapCenter 4.4 e versões posteriores permitem que um usuário não root instale o Pacote de plug-ins do SnapCenter para AIX e inicie o processo de plug-in. Os processos do plug-in serão executados como um usuário não root efetivo. Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se a umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro dela tenham permissão de 555. Caso contrário, a instalação do plug-in poderá falhar.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos do código de autenticação de mensagens: MACs hmac-sha2-256 e MACs hmac-sha2-512.

  Reinicie o serviço sshd após atualizar o arquivo de configuração.

  Exemplo:

```
#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
```

Sobre esta tarefa

Você deve configurar privilégios sudo para que o usuário não root forneça acesso aos seguintes caminhos:

- /home/*AIX_USER*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /localização_personalizada/ NetApp/snapcenter/spl/instalação/plugins/desinstalação
- /localização_personalizada/ NetApp/snapcenter/spl/bin/spl

Passos

1. Efetue login no host AIX no qual você deseja instalar o Pacote de plug-ins do SnapCenter para AIX.
2. Adicione as seguintes linhas ao arquivo /etc/sudoers usando o utilitário visudo Linux.

```
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
```

Se você tiver uma configuração RAC, junto com os outros comandos permitidos, você deve adicionar o seguinte ao arquivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Você pode obter o valor de *crs_home* do arquivo */etc/oracle/olr.loc*.

AIX_USER é o nome do usuário não root que você criou.

Você pode obter o *checksum_value* do arquivo **sc_unix_plugins_checksum.txt**, localizado em:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Linux.

O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows

Antes de instalar o pacote de plug-ins do SnapCenter para Windows, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas Operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	5 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux

Antes de instalar o pacote de plug-ins SnapCenter para Linux, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema

host.

Item	Requisitos
Sistemas operacionais	• Red Hat Enterprise Linux • Servidor SUSE Linux Enterprise (SLES) Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	2 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	Java 11 Oracle Java e OpenJDK Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em /var/opt/snapcenter/spl/etc/spl.properties esteja definida para a versão correta do JAVA e o caminho correto. Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Configurar credenciais para o plug-in SnapCenter para IBM Db2

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter . Você deve criar credenciais para instalar plug-ins do SnapCenter e credenciais adicionais para executar operações de proteção de dados em bancos de dados ou sistemas de arquivos do Windows.

Sobre esta tarefa

- Hosts Linux

Você deve configurar credenciais para instalar plug-ins em hosts Linux.

Você deve configurar as credenciais para o usuário root ou para um usuário não root que tenha privilégios sudo para instalar e iniciar o processo do plug-in.

Melhores práticas: embora você tenha permissão para criar credenciais para o Linux após implantar hosts e instalar plug-ins, a melhor prática é criar credenciais depois de adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

  Você deve configurar as credenciais do Windows antes de instalar plug-ins.

  Você deve configurar as credenciais com privilégios de administrador, incluindo direitos de administrador no host remoto.

Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver privilégios de administrador completos, será necessário atribuir pelo menos os privilégios de grupo de recursos e backup ao nome de usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.
4. Na página Credencial, especifique as informações necessárias para configurar as credenciais:

Para este campo…	Faça isso…
Nome da credencial	Digite um nome para as credenciais.

Para este campo…	Faça isso…
Nome de usuário	Digite o nome de usuário e a senha que serão usados para autenticação. • Administrador de domínio ou qualquer membro do grupo de administradores Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS\Nome do Usuário* ◦ *FQDN do domínio\Nome do usuário* • Administrador local (somente para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é: *UserName* Não use aspas duplas (") ou acento grave (`) nas senhas. Você não deve usar os símbolos de menor que (<) e exclamação (!) juntos em senhas. Por exemplo, menor que <! 10, menor que 10 <!, acento grave `12.
Senha	Digite a senha usada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que você deseja usar.
Use privilégios sudo	Marque a caixa de seleção **Usar privilégios sudo** se estiver criando credenciais para um usuário não root. Aplicável somente a usuários do Linux.

5. Clique em **OK**.

Depois de concluir a configuração das credenciais, talvez você queira atribuir a manutenção de credenciais a um usuário ou grupo de usuários na página Usuário e Acesso.

Configurar o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite que você crie uma Conta de Serviço Gerenciada de grupo (gMSA) que fornece gerenciamento automatizado de senhas de contas de serviço a partir de uma conta de domínio gerenciada.

Antes de começar

- Você deve ter um controlador de domínio do Windows Server 2016 ou posterior.
- Você deve ter um host Windows Server 2016 ou posterior, que seja membro do domínio.

Passos

1. Crie uma chave raiz do KDS para gerar senhas exclusivas para cada objeto no seu gMSA.
2. Para cada domínio, execute o seguinte comando no controlador de domínio do Windows: Add-KDSRootKey -EffectiveImmediately
3. Crie e configure seu gMSA:
   a. Crie uma conta de grupo de usuários no seguinte formato:

```
 domainName\accountName$
.. Adicione objetos de computador ao grupo.
.. Use o grupo de usuários que você acabou de criar para criar o
gMSA.
```

   Por exemplo,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correr `Get-ADServiceAccount` comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Habilite o módulo do Active Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando no PowerShell:

```
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. Reinicie seu host.

b. Instale o gMSA no seu host executando o seguinte comando no prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua privilégios administrativos ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no SnapCenter Server.

   O SnapCenter Server instalará os plug-ins selecionados no host e o gMSA especificado será usado como a conta de logon de serviço durante a instalação do plug-in.

Instalar o plug-in SnapCenter para IBM Db2

Adicionar hosts e instalar pacotes de plug-ins em hosts remotos

Você deve usar a página Adicionar Host do SnapCenter para adicionar hosts e, em seguida, instalar os pacotes de plug-ins. Os plug-ins são instalados automaticamente nos hosts remotos. Você pode adicionar um host e instalar pacotes de plug-in para um host individual ou para um cluster.

Antes de começar

- Se o sistema operacional do host do SnapCenter Server for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deverá executar o seguinte:
  - Atualize para o Windows Server 2019 (versão do sistema operacional 17763.5936) ou posterior
  - Atualize para o Windows Server 2022 (versão do sistema operacional 20348.2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada

ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.

- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- A documentação de administração contém informações sobre o gerenciamento de hosts.
- Se estiver usando uma conta de serviço gerenciada em grupo (gMSA), você deverá configurar a gMSA com privilégios administrativos.

  "Configurar conta de serviço gerenciada de grupo no Windows Server 2016 ou posterior para IBM Db2"

Sobre esta tarefa

- Não é possível adicionar um SnapCenter Server como um host de plug-in a outro SnapCenter Server.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Clique em **Adicionar**.
4. Na página Hosts, execute as seguintes ações:

Para este campo…	Faça isso…
Tipo de host	Selecione o tipo de host: • Windows • Linux O plug-in para IBM Db2 é instalado no host do cliente IBM Db2, e esse host pode estar em um sistema Windows ou Linux.
Nome do host	Digite o nome do host de comunicação. Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o FQDN.

Para este campo…	Faça isso…
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais. Você pode visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial fornecida. O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar Host.

5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a serem instalados.

   Ao usar a API REST para instalar o Plug-in para Db2, você deve passar a versão como 3.0. Por exemplo, Db2:3.0

6. (Opcional) Clique em **Mais opções**.

Para este campo…	Faça isso…
Porta	Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.
Caminho de instalação	O plug-in para IBM Db2 é instalado no host do cliente IBM Db2, e esse host pode estar em um sistema Windows ou Linux. • Para o pacote de plug-ins SnapCenter para Windows, o caminho padrão é C:\Arquivos de Programas\ NetApp\ SnapCenter. Opcionalmente, você pode personalizar o caminho. • Para o pacote de plug-ins SnapCenter para Linux, o caminho padrão é /opt/ NetApp/snapcenter. Opcionalmente, você pode personalizar o caminho.

Para este campo…	Faça isso…
Ignorar verificações de pré-instalação	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.
Use a conta de serviço gerenciada em grupo (gMSA) para executar os serviços do plug-in	Para o host Windows, marque esta caixa de seleção se desejar usar a Conta de Serviço Gerenciada em Grupo (gMSA) para executar os serviços do plug-in. Forneça o nome do gMSA no seguinte formato: domainName\accountName$. O gMSA será usado como uma conta de serviço de logon somente para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

   Se você não tiver marcado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se atende aos requisitos para a instalação do plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão do .NET, a localização (para plug-ins do Windows) e o Java 11 (para plug-ins do Windows e do Linux) são validados em relação aos requisitos mínimos. Se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas serão exibidas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em C:\Arquivos de Programas\ NetApp\ SnapCenter WebApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, deverá atualizar o arquivo em ambos os nós.

8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirmar e Enviar**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós do cluster.

   A verificação de impressão digital é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitore o progresso da instalação.
   - Para o plug-in do Windows, os logs de instalação e atualização estão localizados em: *C:\Windows\ SnapCenter plugin\Install*<JOBID>\
   - Para o plug-in Linux, os logs de instalação estão localizados em: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log e os logs de atualização estão localizados em: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log

Depois que você terminar

Se você quiser atualizar para o SnapCenter 6.0 ou posterior, o plug-in baseado em PERL existente para Db2 será desinstalado do servidor de plug-in remoto.

Instalar pacotes de plug-in SnapCenter para Linux ou Windows em vários hosts remotos usando cmdlets

Você pode instalar os pacotes de plug-in do SnapCenter para Linux ou Windows em vários hosts simultaneamente usando o cmdlet Install-SmHostPackage do PowerShell.

Antes de começar

Você deve ter efetuado login no SnapCenter como um usuário de domínio com direitos de administrador local em cada host no qual deseja instalar o pacote de plug-in.

Passos

1. Inicie o PowerShell.
2. No host do SnapCenter Server, estabeleça uma sessão usando o cmdlet Open-SmConnection e insira suas credenciais.
3. Instale o plug-in em vários hosts usando o cmdlet Install-SmHostPackage e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

   Você pode usar a opção -skipprecheck quando tiver instalado os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

4. Insira suas credenciais para instalação remota.

Instale o plug-in SnapCenter para IBM Db2 em hosts Linux usando a interface de linha de comando

Você deve instalar o SnapCenter Plug-in para IBM Db2 Database usando a interface de usuário (IU) do SnapCenter . Se o seu ambiente não permitir a instalação remota do plug-in a partir da interface do usuário do SnapCenter , você poderá instalar o plug-in para o IBM Db2 Database no modo de console ou no modo silencioso usando a interface de linha de comando (CLI).

Antes de começar

- Você deve instalar o Plug-in para o IBM Db2 Database em cada host Linux onde o cliente IBM Db2 reside.
- O host Linux no qual você está instalando o SnapCenter Plug-in para IBM Db2 Database deve atender aos requisitos de software, banco de dados e sistema operacional dependentes.

  A Ferramenta de Matriz de Interoperabilidade (IMT) contém as informações mais recentes sobre as configurações suportadas.

  "Ferramenta de Matriz de Interoperabilidade da NetApp"

- O plug-in SnapCenter para IBM Db2 Database faz parte do pacote de plug-ins SnapCenter para Linux. Antes de instalar o SnapCenter Plug-ins Package para Linux, você já deve ter instalado o SnapCenter em um host Windows.

Sobre esta tarefa

Se os parâmetros não forem mencionados, o SnapCenter será instalado com valores padrão.

Passos

1. Copie o arquivo de instalação do pacote de plug-ins SnapCenter para Linux (snapcenter_linux_host_plugin.bin) de C:\ProgramData\ NetApp\ SnapCenter\Package Repository para o host onde você deseja instalar o plug-in para IBM Db2.

   Você pode acessar esse caminho a partir do host onde o SnapCenter Server está instalado.

2. No prompt de comando, navegue até o diretório onde você copiou o arquivo de instalação.
3. Instale o plug-in: `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 especifica a porta de comunicação HTTPS do SMCore.
   - -DSERVER_IP especifica o endereço IP do SnapCenter Server.
   - -DSERVER_HTTPS_PORT especifica a porta HTTPS do SnapCenter Server.
   - -DUSER_INSTALL_DIR especifica o diretório onde você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
   - DINSTALL_LOG_NAME especifica o nome do arquivo de log.

   ```
   /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. Edite o arquivo /<diretório de instalação>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties e adicione o parâmetro PLUGINS_ENABLED = DB2:3.0.
5. Adicione o host ao SnapCenter Server usando o cmdlet Add-Smhost e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitore o status da instalação do Plug-in para IBM Db2

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso

- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
   a. Clique em **Filtrar**.
   b. Opcional: especifique a data de início e término.
   c. No menu suspenso Tipo, selecione **Instalação de plug-in**.
   d. No menu suspenso Status, selecione o status da instalação.
   e. Clique em **Aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Configurar certificado CA

Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.

O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte "Como gerar um arquivo CSR de certificado CA" .

Se você possui o certificado CA para seu domínio (*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Importar chave privada	Selecione a opção **Sim**, importe a chave privada e clique em **Avançar**.
Formato de arquivo de importação	Não faça alterações; clique em **Avançar**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

> O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: *.pfx, *.p12 e *.p7b).

7. Repita a Etapa 5 para a pasta “Pessoal”.

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

Passos

1. Execute o seguinte na GUI:
   a. Clique duas vezes no certificado.
   b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.
   c. Percorra a lista de campos e clique em **Impressão digital**.
   d. Copie os caracteres hexadecimais da caixa.
   e. Remova os espaços entre os números hexadecimais.

      Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
   a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copie a impressão digital.

Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Por exemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Vincule o certificado recém-instalado aos serviços de plug-in do host
   do Windows, executando os seguintes comandos:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Por exemplo:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

Configurar o certificado CA para o serviço SnapCenter IBM Db2 Plug-ins no host Linux

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o

serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo 'keystore.jks', que está localizado em */opt/ NetApp/snapcenter/scc/etc* como seu armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in a partir do arquivo de propriedades do agente do plug-in.

   É o valor correspondente à chave 'KEYSTORE_PASS'.

2. Alterar a senha do keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Altere a senha de todos os aliases de entradas de chave privada no
keystore para a mesma senha usada para o keystore:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

   Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

3. Reinicie o serviço após alterar a senha.

> A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Reinicie o serviço após configurar os certificados raiz ou
intermediários para conectar o trust-store.
```

Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Adicione o certificado da CA com chave privada e pública.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Listar os certificados adicionados no keystore.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

   A senha padrão do keystore do plug-in é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Se o nome do alias no certificado da CA for longo e contiver espaços
   ou caracteres especiais ("*",","), altere o nome do alias para um nome
   simples:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configure o nome do alias do certificado CA no arquivo
   agent.properties.
   ```

   Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

Configurar lista de revogação de certificados (CRL) para plug-ins

Sobre esta tarefa

- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.

- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é ' opt/NetApp/snapcenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties em relação à chave CRL_PATH.

   Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Configurar o certificado CA para o serviço SnapCenter IBM Db2 Plug-ins no host Windows

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo *keystore.jks*, que está localizado em *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* como seu armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in a partir do arquivo de propriedades do agente do plug-in.

   É o valor correspondente à chave *KEYSTORE_PASS*.

2. Alterar a senha do keystore:

   keytool -storepasswd -keystore keystore.jks

   > Se o comando "keytool" não for reconhecido no prompt de comando do Windows, substitua o comando keytool pelo seu caminho completo.

   C:\Arquivos de Programas\Java\<versão_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. Altere a senha de todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:

   keytool -keypasswd -alias "nome_do_alias_no_certificado" -keystore keystore.jks

   Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

4. Reinicie o serviço após alterar a senha.

   > A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

   keytool -list -v -keystore keystore.jks

4. Adicione um certificado raiz ou intermediário:

   keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Reinicie o serviço após configurar os certificados raiz ou intermediários para conectar o trust-store.

Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo *keystore.jks*.
3. Listar os certificados adicionados no keystore:

   keytool -list -v -keystore keystore.jks

4. Adicione o certificado da CA com chave privada e pública.

   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS

5. Listar os certificados adicionados no keystore.

   keytool -list -v -keystore keystore.jks

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

   A senha padrão do keystore do plug-in é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

   keytool -keypasswd -alias "nome_do_alias_no_certificado_da_CA" -keystore keystore.jks

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

   Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

Configurar lista de revogação de certificados (CRL) para plug-ins SnapCenter

Sobre esta tarefa

- Para baixar o arquivo CRL mais recente para o certificado CA relacionado, consulte "Como atualizar o arquivo de lista de revogação de certificados no SnapCenter CA Certificate" .
- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é *'C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo *agent.properties* em relação à chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

   Os certificados recebidos serão verificados em relação a cada CRL.

Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *Get-SmCertificateSettings*.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- * * indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- * * indica que o certificado CA foi validado com sucesso.
- * * indica que o certificado CA não pôde ser validado.
- * * indica que as informações de conexão não puderam ser recuperadas.

Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Prepare-se para a proteção de dados

Pré-requisitos para usar o plug-in SnapCenter para IBM Db2

Antes de usar o SnapCenter Plug-in para IBM Db2, o administrador do SnapCenter deve instalar e configurar o SnapCenter Server e executar as tarefas de pré-requisito.

- Instalar e configurar o SnapCenter Server.
- Efetue login no SnapCenter Server.
- Configure o ambiente SnapCenter adicionando conexões do sistema de armazenamento e criando credenciais, se aplicável.
- Instale o Java 11 no seu host Linux ou Windows.

  Você deve definir o caminho Java na variável de caminho ambiental da máquina host.

- Configure o SnapMirror e o SnapVault se desejar replicação de backup.

Como recursos, grupos de recursos e políticas são usados para proteger o IBM Db2

Antes de usar o SnapCenter, é útil entender os conceitos básicos relacionados às operações de backup, clonagem e restauração que você deseja executar. Você interage com recursos, grupos de recursos e políticas para diferentes operações.

- Os recursos geralmente são bancos de dados IBM Db2 que você faz backup ou clona com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host.

  Ao executar uma operação em um grupo de recursos, você executa essa operação nos recursos definidos no grupo de recursos de acordo com o cronograma especificado para o grupo de recursos.

  Você pode fazer backup sob demanda de um único recurso ou de um grupo de recursos. Você também pode executar backups agendados para recursos individuais e grupos de recursos.

- As políticas especificam a frequência de backup, replicação, scripts e outras características das operações de proteção de dados.

  Ao criar um grupo de recursos, você seleciona uma ou mais políticas para esse grupo. Você também pode selecionar uma política ao executar um backup sob demanda para um único recurso.

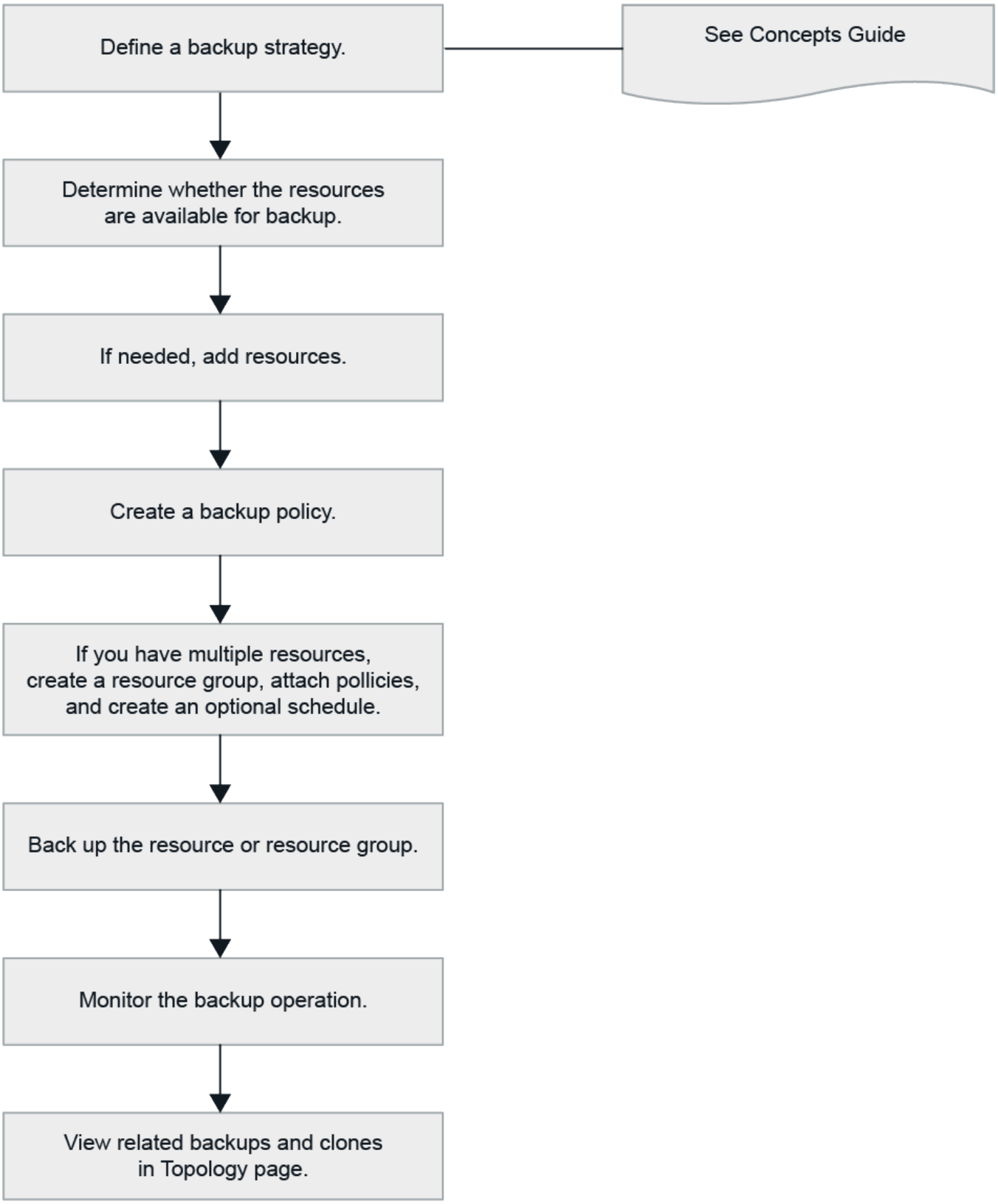
Pense em um grupo de recursos como algo que define o que você quer proteger e quando quer proteger em termos de dia e hora. Pense em uma política como a definição de como você deseja protegê-la. Se você estiver fazendo backup de todos os bancos de dados, por exemplo, poderá criar um grupo de recursos que inclua todos os bancos de dados no host. Você pode então anexar duas políticas ao grupo de recursos: uma política diária e uma política horária. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diariamente.

Fazer backup dos recursos do IBM Db2

Fazer backup dos recursos do IBM Db2

Você pode criar um backup de um recurso (banco de dados) ou grupo de recursos. O fluxo de trabalho de backup inclui planejamento, identificação dos bancos de dados para backup, gerenciamento de políticas de backup, criação de grupos de recursos e anexação de políticas, criação de backups e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de backup:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell. "Guia de referência do cmdlet do software SnapCenter" .

Descubra os bancos de dados automaticamente

Os recursos são bancos de dados IBM Db2 no host Linux que são gerenciados pelo SnapCenter. Você pode adicionar os recursos aos grupos de recursos para executar operações de proteção de dados depois de descobrir os bancos de dados IBM Db2 que estão disponíveis.

Antes de começar

- Você já deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts e configurar as conexões do sistema de armazenamento.
- O plug-in SnapCenter para IBM Db2 não oferece suporte à descoberta automática de recursos que residem em ambientes virtuais RDM/VMDK. Você deve fornecer as informações de armazenamento para ambientes virtuais ao adicionar os bancos de dados manualmente.

Sobre esta tarefa

- Após instalar o plug-in, todos os bancos de dados naquele host Linux são descobertos automaticamente e exibidos na página Recursos.
- Somente bancos de dados são descobertos automaticamente.

Os recursos descobertos automaticamente não podem ser modificados ou excluídos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o Plug-in para IBM Db2 na lista.
2. Na página Recursos, selecione o tipo de recurso na lista Exibir.
3. (Opcional) Clique em * * e, em seguida, selecione o nome do host.

   Você pode então clicar em * * para fechar o painel de filtro.

4. Clique em **Atualizar recursos** para descobrir os recursos disponíveis no host.

   Os recursos são exibidos junto com informações como tipo de recurso, nome do host, grupos de recursos associados, tipo de backup, políticas e status geral.

   - Se o banco de dados estiver em um armazenamento NetApp e não estiver protegido, Não protegido será exibido na coluna Status geral.
   - Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, e se nenhuma operação de backup for realizada, Backup não executado será exibido na coluna Status geral. Caso contrário, o status mudará para Falha no backup ou Backup bem-sucedido com base no último status do backup.

Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

Adicionar recursos manualmente ao host do plug-in

A descoberta automática não é suportada no host Windows. Você deve adicionar instâncias do Db2 e recursos de banco de dados manualmente.

Antes de começar

- Você deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts e configurar conexões do sistema de armazenamento.

Sobre esta tarefa

A descoberta manual não é suportada para as seguintes configurações:

- Layouts RDM e VMDK

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o SnapCenter Plug-in para IBM Db2 na lista suspensa.
2. Na página Recursos, clique em **Adicionar recurso IBM DB2**.
3. Na página Fornecer detalhes do recurso, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Especifique o nome do banco de dados.
Nome do host	Digite o nome do host.
Tipo	Selecione o banco de dados ou instância.
Exemplo	Especifique o nome da instância, que é o pai do banco de dados.
Credenciais	Selecione as credenciais ou adicione informações para a credencial. Isto é opcional.

4. Na página Fornecer espaço de armazenamento, selecione um tipo de armazenamento e escolha um ou mais volumes, LUNs e qtrees e clique em **Salvar**.

   Opcional: Você pode clicar no *  * ícone para adicionar mais volumes, LUNs e qtrees de outros sistemas de armazenamento.

5. Opcional: Na página Configurações de Recursos, para recursos no host do Windows, insira pares de chave-valor personalizados para o plug-in IBM Db2
6. Revise o resumo e clique em **Concluir**.

   Os bancos de dados são exibidos junto com informações como o nome do host, grupos de recursos e políticas associados e status geral

Se você quiser fornecer aos usuários acesso aos recursos, deverá atribuir os recursos aos usuários. Isso permite que os usuários executem as ações para as quais têm permissão nos ativos atribuídos a eles.

"Adicionar um usuário ou grupo e atribuir função e ativos"

Depois de adicionar os bancos de dados, você pode modificar os detalhes do banco de dados IBM Db2.

Criar políticas de backup para IBM Db2

Antes de usar o SnapCenter para fazer backup de recursos do IBM Db2, você deve criar uma política de backup para o recurso ou grupo de recursos do qual deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e mantém backups.

Antes de começar

- Você deve ter definido sua estratégia de backup.

  Para obter detalhes, consulte as informações sobre como definir uma estratégia de proteção de dados para bancos de dados IBM Db2.

- Você deve ter se preparado para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, configurar conexões do sistema de armazenamento e adicionar recursos.
- O administrador do SnapCenter deve ter atribuído as SVMs para os volumes de origem e destino a você se estiver replicando instantâneos para um espelho ou cofre.

  Além disso, você pode especificar configurações de replicação, script e aplicativo na política. Essas opções economizam tempo quando você deseja reutilizar a política para outro grupo de recursos.

Sobre esta tarefa

- SnapLock
  - Se a opção 'Manter as cópias de backup por um número específico de dias' for selecionada, o período de retenção do SnapLock deverá ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio de instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar à retenção de um número maior de instantâneos do que a contagem especificada na política.
  - Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Clique em **Novo**.
4. Na página Nome, insira o nome e os detalhes da política.
5. Na página Tipo de política, faça o seguinte:
   a. Selecione o tipo de armazenamento.
   b. Na seção **Configurações de backup personalizadas**, forneça quaisquer configurações de backup específicas que devem ser passadas ao plug-in no formato chave-valor.

      Você pode fornecer vários valores-chave a serem passados ao plug-in.

6. Na página Snapshot e Replicação, execute as seguintes ações.

   a. Especifique a frequência da programação selecionando **Sob demanda**, **Por hora**, **Diariamente**, **Semanalmente** ou **Mensalmente**.

Você pode especificar o agendamento (data de início, data de término e frequência) para a operação de backup ao criar um grupo de recursos. Isso permite que você crie grupos de recursos que compartilham a mesma política e frequência de backup, mas também permite que você atribua diferentes agendamentos de backup a cada política.

Se você agendou para 2h00, a programação não será acionada durante o horário de verão (DST).

a. Na seção Configurações do Snapshot, execute as seguintes ações:

Se você quiser…	Então…
Mantenha um certo número de instantâneos	Selecione **Cópias a serem mantidas** e especifique o número de instantâneos que você deseja manter. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos, com as cópias mais antigas sendo excluídas primeiro.
Mantenha os Snapshots por um certo número de dias	Selecione **Manter cópias por** e especifique o número de dias pelos quais você deseja manter os Snapshots antes de excluí-los.
Período de bloqueio de cópia de instantâneo	Selecione **Período de bloqueio de cópia de instantâneo** e especifique dias, meses ou anos. O período de retenção do Snaplock deve ser inferior a 100 anos.

Para backups baseados em cópia de instantâneo, você deve definir a contagem de retenção como 2 ou mais se planeja habilitar a replicação do SnapVault . Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro instantâneo será o instantâneo de referência para o relacionamento SnapVault até que um instantâneo mais recente seja replicado para o destino.

b. Especifique o rótulo da política.

Você pode atribuir rótulos SnapMirror a snapshots primários para replicação remota, permitindo que os snapshots primários descarreguem a operação de replicação de snapshots do SnapCenter para sistemas secundários ONTAP . Isso pode ser feito sem habilitar a opção SnapMirror ou SnapVault na página de política.

7. Na seção Selecionar opções de replicação secundária, selecione uma ou ambas as seguintes opções de replicação secundária:

Para este campo…	Faça isso…
Atualizar o SnapMirror após criar uma cópia local do Snapshot	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Esta opção deve ser habilitada para sincronização ativa do SnapMirror .
Atualizar o SnapVault após criar uma cópia local do Snapshot	Selecione esta opção para executar a replicação de backup de disco para disco (backups do SnapVault).
Contagem de novas tentativas de erro	Insira o número máximo de tentativas de replicação que podem ser permitidas antes que a operação seja interrompida.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o armazenamento secundário para evitar atingir o limite máximo de Snapshots no armazenamento secundário.

8. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas

Um grupo de recursos é o contêiner ao qual você deve adicionar recursos que deseja fazer backup e proteger. Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente. Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que deseja executar.

Sobre esta tarefa

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Insira um nome para o grupo de recursos. O nome do grupo de recursos não deve exceder 250 caracteres.

Para este campo…	Faça isso…
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.
Use formato de nome personalizado para cópia de instantâneo	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do instantâneo. Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do instantâneo.

4. Na página Recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Tipo de recurso**.

   Isso ajuda a filtrar informações na tela.

5. Selecione os recursos na seção **Recursos disponíveis** e clique na seta para a direita para movê-los para a seção **Recursos selecionados**.
6. Na página Configurações do aplicativo, faça o seguinte:

   a. Clique na seta **Backups** para definir opções adicionais de backup:

      Habilite o backup do grupo de consistência e execute as seguintes tarefas:

Para este campo…	Faça isso…
Permitir tempo para esperar a conclusão da operação de instantâneo do Consistency Group	Selecione **Urgente**, **Médio** ou **Relaxado** para especificar o tempo de espera para a conclusão da operação de instantâneo. Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.
Desativar sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL .

+

a. Clique na seta **Scripts** e insira os comandos pre e post para operações de inatividade, snapshot e unquiesce. Você também pode inserir os pré-comandos a serem executados antes de sair em caso de falha.

b. Clique na seta **Configurações personalizadas** e insira os pares de chave-valor personalizados necessários para todas as operações de proteção de dados que usam este recurso.

Parâmetro	Contexto	Descrição
HABILITAR_REGISTRO_DE_ARQUIVO	(S/N)	Permite que o gerenciamento de log de arquivamento exclua os logs de arquivamento.
RETENÇÃO_DE_REGISTRO_DE_ARQUIVO	número_de_dias	Especifica o número de dias que os logs de arquivamento são retidos. Esta configuração deve ser igual ou maior que NTAP_SNAPSHOT_RETENTIONS.
DIRETÓRIO_DE_LOG_DE_ARQUIVO	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs de arquivamento.

Parâmetro	Contexto	Descrição
EXT_DE_LOG_DE_ARQUIVO	extensão_de_arquivo	Especifica o comprimento da extensão do arquivo de log de arquivamento. Por exemplo, se o log de arquivamento for log_backup_0_0_0_0.16151855 1942 9 e se o valor file_extension for 5, a extensão do log manterá 5 dígitos, que é 16151.
ARQUIVO_LOG_RECURSIVO_ SE ARQUIVO	(S/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs de arquivamento estiverem localizados em subdiretórios.

Os pares de chave-valor personalizados são suportados para sistemas de plug-in IBM Db2 Linux e não são suportados para o banco de dados IBM Db2 registrado como um plug-in centralizado do Windows.

c. Clique na seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar instantâneos:

Se você quiser…	Então…
SnapCenter para usar o plug-in para Windows e colocar o sistema de arquivos em um estado consistente antes de criar um snapshot. Para recursos do Linux, esta opção não é aplicável.	Selecione * SnapCenter com consistência do sistema de arquivos*.
SnapCenter para criar um instantâneo de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.
Para inserir o comando a ser executado no host para criar cópias de instantâneos.	Selecione **Outro** e insira o comando a ser executado no host para criar um instantâneo.

7. Na página Políticas, execute as seguintes etapas:

a. Selecione uma ou mais políticas na lista suspensa.

Você também pode criar uma política clicando em * + *.

As políticas são listadas na seção Configurar agendamentos para políticas selecionadas.

b. Na coluna Configurar agendamentos, clique em * + * para a política que você deseja configurar.

c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

Onde policy_name é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna **Agendamentos Aplicados**.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. O servidor SMTP deve ser configurado em **Configurações** > **Configurações globais**.

9. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e habilite proteção secundária para recursos do IBM Db2 em sistemas ASA r2

Você deve criar o grupo de recursos para adicionar os recursos que estão nos sistemas ASA r2. Você também pode provisionar a proteção secundária ao criar o grupo de recursos.

Antes de começar

- Você deve garantir que não está adicionando recursos do ONTAP 9.x e recursos do ASA r2 ao mesmo grupo de recursos.
- Você deve garantir que não tenha um banco de dados com recursos ONTAP 9.x e recursos ASA r2.

Sobre esta tarefa

- A proteção secundária estará disponível somente se o usuário conectado estiver atribuído à função que tem o recurso **SecondaryProtection** habilitado.
- Se você habilitar a proteção secundária, o grupo de recursos será colocado no modo de manutenção durante a criação dos grupos de consistência primário e secundário. Depois que os grupos de consistência primário e secundário são criados, o grupo de recursos é retirado do modo de manutenção.
- O SnapCenter não oferece suporte à proteção secundária para um recurso clone.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:
   a. Insira um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 caracteres.

   b. Insira um ou mais rótulos no campo Tag para ajudar você a pesquisar o grupo de recursos posteriormente.

Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.

c. Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

d. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

Você deve usar exatamente o mesmo destino definido no aplicativo, incluindo o prefixo, se necessário.

4. Na página Recursos, selecione o nome do host do banco de dados na lista suspensa **Host**.

Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos do ASA r2 na seção Recursos disponíveis e mova-os para a seção Recursos selecionados.
6. Na página Configurações do aplicativo, selecione a opção de backup.
7. Na página Políticas, execute as seguintes etapas:

a. Selecione uma ou mais políticas na lista suspensa.

Você também pode criar uma política clicando em + .

Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

Onde *policy_name* é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Se a proteção secundária estiver habilitada para a política selecionada, a página Proteção Secundária será exibida e você precisará executar as seguintes etapas:

a. Selecione o tipo de política de replicação.

A política de replicação síncrona não é suportada.

b. Especifique o sufixo do grupo de consistência que você deseja usar.

c. Nos menus suspensos Cluster de destino e SVM de destino, selecione o cluster emparelhado e o SVM que você deseja usar.

> O cluster e o peering de SVM não são suportados pelo SnapCenter. Você deve usar o System Manager ou as CLIs do ONTAP para executar o peering de cluster e SVM.

> Se os recursos já estiverem protegidos fora do SnapCenter, eles serão exibidos na seção Recursos Protegidos Secundários.

1. Na página Verificação, execute as seguintes etapas:

   a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para realizar a verificação no armazenamento secundário.

   b. Clique + na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política.

   c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name, execute as seguintes ações:

Se você quiser…	Faça isso…
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

   d. Selecione **Verificar no local secundário** para verificar seus backups no sistema de armazenamento secundário.

   e. Clique em **OK**.

   Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

2. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

   > Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

3. Revise o resumo e clique em **Concluir**.

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para IBM Db2

Você deve criar uma conexão de máquina virtual de armazenamento (SVM) e uma

credencial antes de usar cmdlets do PowerShell para fazer backup, restaurar ou clonar bancos de dados IBM Db2.

Antes de começar

- Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.
- Você deve ter as permissões necessárias na função de administrador de infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estejam em andamento.

  As instalações do plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento porque o cache do host pode não ser atualizado e o status dos bancos de dados pode ser exibido na GUI do SnapCenter como “Não disponível para backup” ou "`Não no armazenamento NetApp ".

- Os nomes dos sistemas de armazenamento devem ser exclusivos.

  O SnapCenter não oferece suporte a vários sistemas de armazenamento com o mesmo nome em clusters diferentes. Cada sistema de armazenamento suportado pelo SnapCenter deve ter um nome exclusivo e um endereço IP LIF de dados exclusivo.

Passos

1. Clique em **SnapCenterPS** para iniciar o PowerShell Core.
2. Crie uma nova conexão com o sistema de armazenamento usando o cmdlet Add-SmStorageConnection.

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

3. Crie uma nova credencial usando o cmdlet Add-SmCredential.

   Este exemplo mostra como criar uma nova credencial chamada FinanceAdmin com credenciais do Windows:

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

4. Adicione o host de comunicação IBM Db2 ao SnapCenter Server.

   Para Linux:

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

   Para Windows:

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

5. Instale o pacote e o plug-in SnapCenter para IBM Db2 no host.

   Para Linux:

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

   Para Windows:

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

6. Defina o caminho para o SQLLIB.

   Para Windows, o plug-in Db2 usará o caminho padrão para a pasta SQLLIB: “C:\Arquivos de Programas\IBM\SQLLIB\BIN”

   Se você quiser substituir o caminho padrão, use o seguinte comando.

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

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup de bancos de dados Db2

Fazer backup de um banco de dados inclui estabelecer uma conexão com o SnapCenter Server, adicionar recursos, adicionar uma política, criar um grupo de recursos de backup e fazer backup.

Antes de começar

- Você deve ter criado uma política de backup.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.
- Para a operação de backup baseada em cópia de instantâneo, certifique-se de que todos os bancos de dados de locatários sejam válidos e ativos.

- Para comandos pré e pós para operações de inatividade, instantâneo e retomada de atividade, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recurso, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Selecione e selecione o nome do host e o tipo de recurso para filtrar os recursos. Você pode então selecionar para fechar o painel de filtro.
3. Selecione o recurso que você deseja fazer backup.
4. Na página Recurso, selecione **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.
5. Na página Configurações do aplicativo, faça o seguinte:
   - Selecione a seta **Backups** para definir opções adicionais de backup:

     Habilite o backup do grupo de consistência, se necessário, e execute as seguintes tarefas:

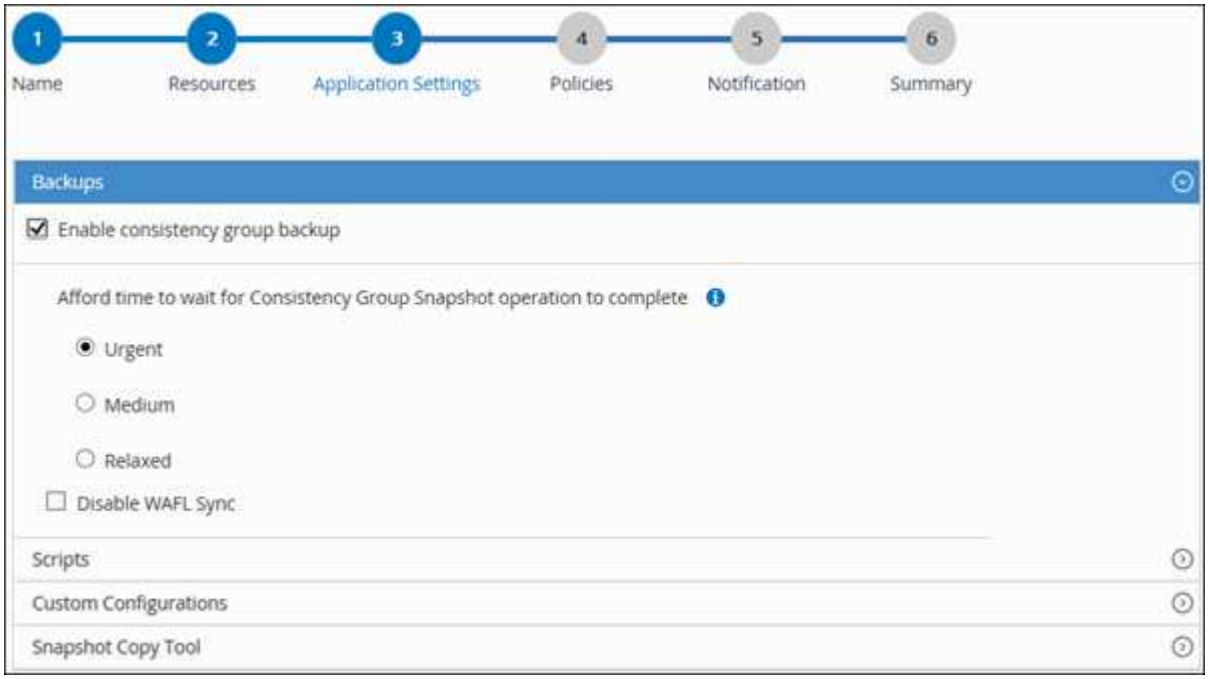
Para este campo…	Faça isso…
Permitir tempo para esperar a conclusão da operação "Consistency Group Snapshot"	Selecione **Urgente**, ou **Médio**, ou **Relaxado** para especificar o tempo de espera para a operação de Snapshot terminar. Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.
Desativar sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL .

   - Selecione a seta **Scripts** para executar comandos pré e pós para operações de inatividade, instantâneo e ativação/desativação.

     Você também pode executar pré-comandos antes de sair da operação de backup. Prescrições e pós-escritos são executados no SnapCenter Server.
   - Selecione a seta **Configurações personalizadas** e insira os pares de valores personalizados necessários para todos os trabalhos que usam este recurso.
   - Selecione a seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar Instantâneos:

Se você quiser…	Então…
SnapCenter para criar um Snapshot de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.

Se você quiser…	Então…
SnapCenter para usar o plug-in para Windows para colocar o sistema de arquivos em um estado consistente e, em seguida, criar um Snapshot	Selecione * SnapCenter com consistência do sistema de arquivos*.
Para inserir o comando para criar um Snapshot	Selecione **Outro** e insira o comando para criar um Snapshot.



6. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em * + *.

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Selecione * + * na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

   c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione **OK**.

      policy_name é o nome da política que você selecionou.

   Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

7. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. O SMTP também deve ser configurado em **Configurações** > **Configurações globais**.

8. Revise o resumo e selecione **Concluir**.

   A página de topologia de recursos é exibida.

9. Selecione **Fazer backup agora**.
10. Na página Backup, execute as seguintes etapas:
    a. Se você aplicou várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

       Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

    b. Selecione **Backup**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.
    - Nas configurações do MetroCluster , o SnapCenter pode não conseguir detectar um relacionamento de proteção após um failover.

      Para mais informações, consulte: "Não é possível detectar o relacionamento SnapMirror ou SnapVault após failover do MetroCluster"

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

   O prompt de nome de usuário e senha é exibido.

2. Adicione recursos manuais usando o cmdlet Add-SmResources.

   Este exemplo mostra como adicionar uma instância do IBM Db2:

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

   Para banco de dados Db2:

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

3. Crie uma política de backup usando o cmdlet Add-SmPolicy.
4. Proteja o recurso ou adicione um novo grupo de recursos ao SnapCenter usando o cmdlet Add-SmResourceGroup.
5. Inicie uma nova tarefa de backup usando o cmdlet New-SmBackup.

   Este exemplo mostra como fazer backup de um grupo de recursos:

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

   Este exemplo faz backup de uma instância do Db2:

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

   Este exemplo faz backup de um banco de dados Db2:

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

6. Monitore o status do trabalho (em execução, concluído ou com falha) usando o cmdlet Get-smJobSummaryReport.

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

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

7. Monitore os detalhes do trabalho de backup, como ID do backup, nome do backup para executar a operação de restauração ou clonagem usando o cmdlet Get-SmBackupReport.

```
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
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup de grupos de recursos

Um grupo de recursos é uma coleção de recursos em um host. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos.

Antes de começar

- Você deve ter criado um grupo de recursos com uma política anexada.

- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.

Sobre esta tarefa

Você pode fazer backup de um grupo de recursos sob demanda na página Recursos. Se um grupo de recursos tiver uma política anexada e um agendamento configurado, os backups ocorrerão automaticamente de acordo com o agendamento.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.

   Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou selecionando e, em seguida, selecionando a tag. Você pode então selecionar para fechar o painel de filtro.

3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e selecione **Fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
   a. Se você associou várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

      Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

   b. Selecione **Backup**.
5. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Monitorar operações de backup do IBM Db2

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Talvez você queira verificar o progresso para determinar quando ele foi concluído ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado correspondente das operações:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **Trabalhos**.
3. Na página Trabalhos, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de backup sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Backup**.
   d. No menu suspenso **Status**, selecione o status do backup.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione uma tarefa de backup e clique em **Detalhes** para visualizar os detalhes da tarefa.

   Embora o status do trabalho de backup seja exibido , ao clicar em detalhes do trabalho, você poderá ver que algumas das tarefas filhas da operação de backup ainda estão em andamento ou marcadas com sinais de alerta.

5. Na página Detalhes do trabalho, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Monitore as operações de proteção de dados em bancos de dados IBM Db2 no painel Atividade

O painel Atividade exibe as cinco operações mais recentes realizadas. O painel Atividade também exibe quando a operação foi iniciada e o status da operação.

O painel Atividade exibe informações sobre operações de backup, restauração, clonagem e backup agendado.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Clique no painel Atividade para visualizar as cinco operações mais recentes.

   Quando você clica em uma das operações, os detalhes da operação são listados na página **Detalhes do trabalho**.

Cancelar operações de backup para IBM Db2

Você pode cancelar operações de backup que estão na fila.

O que você vai precisar

- Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de backup em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de backup.

- O botão **Cancelar trabalho** fica desabilitado para operações que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de backup enfileiradas de outros membros enquanto estiver usando essa função.

Passos

1. Execute uma das seguintes ações:

Do…	Ação
Página do monitor	a. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. b. Selecione a operação e clique em **Cancelar trabalho**.
Painel de atividades	a. Após iniciar a operação de backup, clique em * * no painel Atividade para visualizar as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

A operação é cancelada e o recurso é revertido ao estado anterior.

Visualizar backups e clones do IBM Db2 na página Topologia

Ao se preparar para fazer backup ou clonar um recurso, pode ser útil visualizar uma representação gráfica de todos os backups e clones no armazenamento primário e secundário.

Sobre esta tarefa

Você pode revisar os seguintes ícones na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no armazenamento primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups e clones que estão disponíveis no armazenamento primário.
- exibe o número de backups e clones que são espelhados no armazenamento secundário usando a tecnologia SnapMirror .
- exibe o número de backups e clones que são replicados no armazenamento secundário usando a tecnologia SnapVault .

O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou 6 backups usando uma política para manter apenas 4 backups, o número de backups exibidos será 6.

Clones de um backup de um espelho flexível em termos de versão em um volume do tipo mirror-vault são exibidos na exibição de topologia, mas a contagem de backups de espelho na exibição de topologia não inclui o backup flexível em termos de versão.

Na página Topologia, você pode ver todos os backups e clones disponíveis para o recurso ou grupo de recursos selecionado. Você pode visualizar os detalhes desses backups e clones e selecioná-los para executar operações de proteção de dados.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso na exibição de detalhes do recurso ou na exibição de detalhes do grupo de recursos.

   Se o recurso estiver protegido, a página de topologia do recurso selecionado será exibida.

4. Revise o **cartão Resumo** para ver um resumo do número de backups e clones disponíveis no armazenamento primário e secundário.

   A seção **Cartão de resumo** exibe o número total de backups baseados em cópias de instantâneo e clones.

   Clicar no botão **Atualizar** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clicar no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Uma programação semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo estiver distribuído em vários volumes, o tempo de expiração do SnapLock para o backup será o maior tempo de expiração do SnapLock definido para um Snapshot em um volume. O maior tempo de expiração do SnapLock é recuperado do ONTAP.

   Após o backup sob demanda, clicar no botão **Atualizar** atualiza os detalhes do backup ou clone.

5. Na exibição Gerenciar cópias, clique em **Backups** ou **Clones** do armazenamento primário ou secundário para ver detalhes de um backup ou clone.

   Os detalhes dos backups e clones são exibidos em formato de tabela.

6. Selecione o backup na tabela e clique nos ícones de proteção de dados para executar operações de restauração, clonagem e exclusão.

   Não é possível renomear ou excluir backups que estejam no armazenamento secundário.

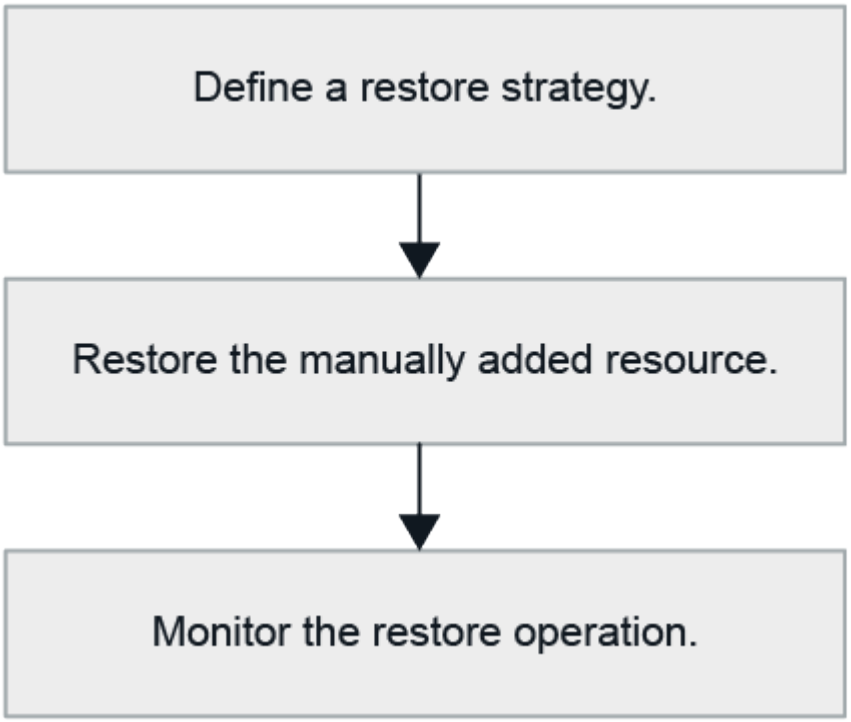
7. Se você quiser excluir um clone, selecione o clone na tabela e clique em  .
8. Se você quiser dividir um clone, selecione o clone na tabela e clique em  .

Restaurar IBM Db2

Fluxo de trabalho de restauração

O fluxo de trabalho de restauração e recuperação inclui planejamento, execução de operações de restauração e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de restauração:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre os cmdlets do PowerShell.

"Guia de referência do cmdlet do software SnapCenter" .

Restaurar um backup de recurso adicionado manualmente

Você pode usar o SnapCenter para restaurar e recuperar dados de um ou mais backups.

Antes de começar

- Você deve ter feito backup do recurso ou dos grupos de recursos.
- Você deve ter cancelado qualquer operação de backup que esteja em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos de pré-restauração, pós-restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com o tipo, host, grupos de recursos e políticas associados e status.

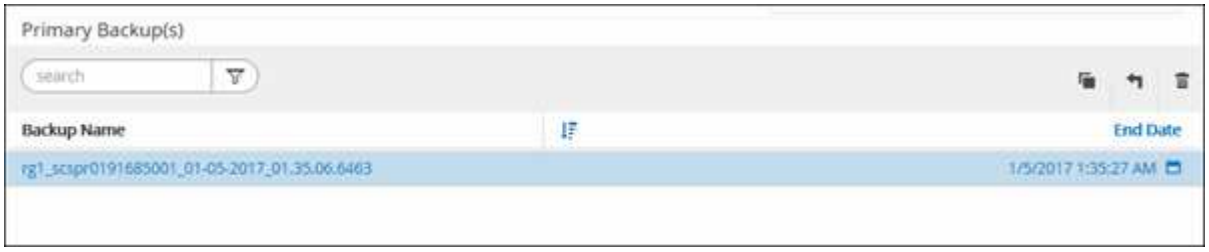
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, “Não protegido” será exibido na coluna Status geral. Isso pode significar que o recurso não está protegido ou que o backup do recurso foi feito por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e depois selecione um recurso nesse grupo.

   A página de topologia de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela Backup(s) primário(s), selecione o backup que deseja restaurar e clique em *  *.



6. Na página Escopo de restauração, selecione **Recurso completo**.

   a. Se você selecionar **Recurso Completo**, todos os volumes de dados configurados do banco de dados IBM Db2 serão restaurados.

      Se o recurso contiver volumes ou qtrees, os Snapshots tirados após o Snapshot selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

      Você pode selecionar vários LUNs.

      Se você selecionar **Todos**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.

7. Na página Pré-operações, insira os comandos pre restore e unmount para executar antes de realizar um trabalho de restauração.
8. Na página Post ops, insira os comandos mount e post restore para serem executados após realizar um trabalho de restauração.
9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais

você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O SMTP também deve ser configurado na página **Configurações** > **Configurações globais**.

10. Revise o resumo e clique em **Concluir**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Depois que você terminar

A recuperação só é possível se o status do Rollforward estiver em "BD pendente". Este status é aplicável a bancos de dados Db2 com registro de arquivamento habilitado.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

2. Identifique o backup que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo mostra que há dois backups disponíveis para a restauração:

```
 PS C:\> Get-SmBackup -AppObjectId
cn24.sccore.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
```

   Este exemplo exibe informações detalhadas sobre o backup de 29 de janeiro de 2015 a 3 de fevereiro de 2015:

```
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. Restaure os dados do backup usando o cmdlet Restore-SmBackup.

> AppObjectId é "Host\Plugin\UID", onde UID = <nome_da_instância> é para o recurso de instância do DB2 descoberto manualmente e UID = <nome_da_instância>\<nome_do_banco_de_dados> é para o recurso de banco de dados IBM Db2. Você pode obter o ResourceID no cmdlet Get-smResources.

```
Get-smResources  -HostName cn24.sccore.test.com  -PluginCode DB2
```

Este exemplo mostra como restaurar o banco de dados do armazenamento primário:

```
Restore-SmBackup -PluginCode DB2 -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\DB01 -BackupId 3
```

Este exemplo mostra como restaurar o banco de dados do armazenamento secundário:

```
Restore-SmBackup -PluginCode 'DB2' -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false
-Archive @( @{"Primary"="<Primary
Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
Vserver>:<SecondaryVolume>"})
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Restaurar e recuperar um backup de banco de dados descoberto automaticamente

Você pode usar o SnapCenter para restaurar e recuperar dados de um ou mais backups.

Antes de começar

- Você deve ter feito backup do recurso ou dos grupos de recursos.
- Você deve ter cancelado qualquer operação de backup que esteja em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos de pré-restauração, pós-restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Para recursos descobertos automaticamente, a restauração é suportada com SFSR.
- A recuperação automática não é suportada.
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com o tipo, host, grupos de recursos e políticas associados e status.

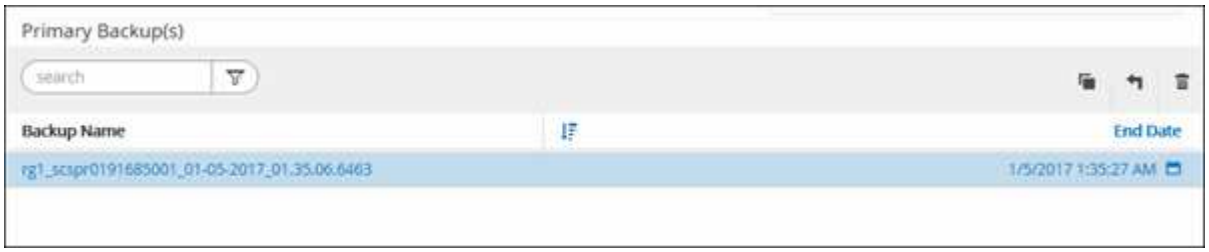
Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

Se o recurso não estiver protegido, “Não protegido” será exibido na coluna Status geral. Isso pode significar que o recurso não está protegido ou que o backup do recurso foi feito por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e depois selecione um recurso nesse grupo.

   A página de topologia de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela Backup(s) primário(s), selecione o backup que deseja restaurar e clique em *  *.



6. Na página Escopo de restauração, selecione **Recurso completo** para restaurar os volumes de dados configurados do banco de dados IBM Db2.
7. Na página Pré-operações, insira os comandos pre restore e unmount para executar antes de realizar um trabalho de restauração.

   Comandos de desmontagem não são necessários para recursos descobertos automaticamente.

8. Na página Post ops, insira os comandos mount e post restore para serem executados após realizar um trabalho de restauração.

   Comandos de montagem não são necessários para recursos descobertos automaticamente.

9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O SMTP também deve ser configurado na página **Configurações** > **Configurações globais**.

10. Revise o resumo e clique em **Concluir**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Depois que você terminar

A recuperação só é possível se o status do Rollforward estiver em "BD pendente". Este status é aplicável a bancos de dados Db2 com registro de arquivamento habilitado.

Monitorar operações de restauração do IBM Db2

Você pode monitorar o progresso de diferentes operações de restauração do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma

operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa tomar.

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de restauração sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Restaurar**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Aplicar** para visualizar as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Clonar backups de recursos do IBM Db2

Fluxo de trabalho de clonagem

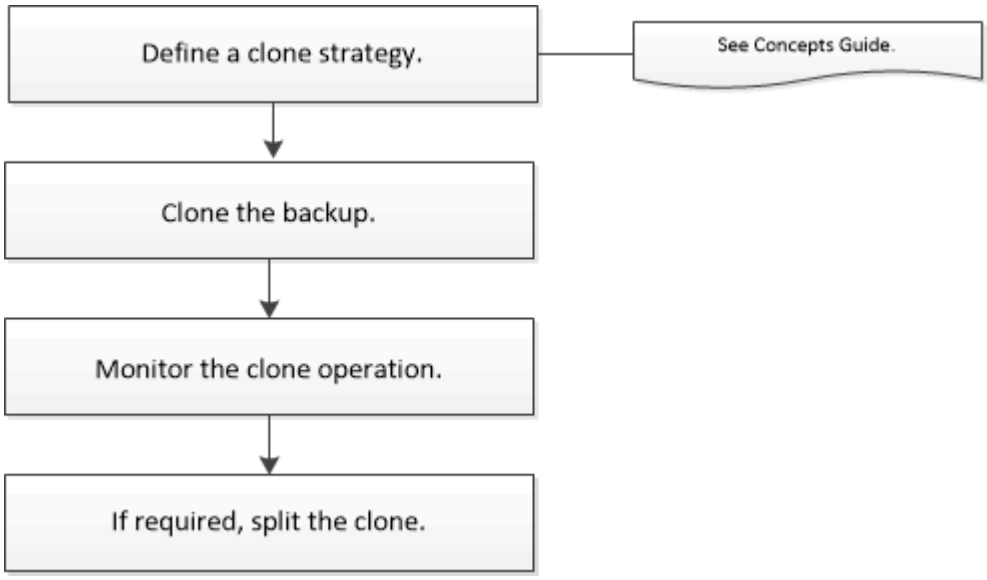
O fluxo de trabalho de clonagem inclui executar a operação de clonagem e monitorar a operação.

Sobre esta tarefa

- Você pode clonar no servidor IBM Db2 de origem.
- Você pode clonar backups de recursos pelos seguintes motivos:
  - Para testar a funcionalidade que deve ser implementada usando a estrutura e o conteúdo atuais dos recursos durante os ciclos de desenvolvimento do aplicativo
  - Para ferramentas de extração e manipulação de dados ao preencher data warehouses

◦ Para recuperar dados que foram excluídos ou alterados por engano

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de clonagem:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre os cmdlets do PowerShell.

Depois que você terminar

Após clonar os recursos do Db2 descobertos automaticamente, o recurso clonado é marcado como recurso manual. Clique em **Atualizar recursos** para recuperar o recurso Db2 clonado. Quando você exclui o clone, o armazenamento e o host também são limpos.

Se você não atualizar os recursos após a operação de clonagem e tentar excluir o clone, o armazenamento e o host não serão limpos. Você deve excluir as entradas manualmente no fstab.

Clonar um backup do IBM Db2

Você pode usar o SnapCenter para clonar um backup. Você pode clonar a partir do backup primário ou secundário.

Antes de começar

- Você deve ter feito backup dos recursos ou do grupo de recursos.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de armazenamento (SVM).
- Ao criar um clone para o Db2 em um host alternativo, você deve criar uma estrutura de diretório n-1 para o caminho de montagem do clone, igual ao caminho de montagem original no outro host. O caminho de montagem deve ter permissão de execução *755*.
- Para comandos de pré-clonagem ou pós-clonagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Para obter informações sobre as operações de divisão de volume do FlexClone , consultehttps://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html["Dividir um volume FlexClone de seu volume pai"] .
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com informações como tipo, host, grupos de recursos e políticas associados e status.

3. Selecione o recurso ou grupo de recursos.

   Você deve selecionar um recurso se selecionar um grupo de recursos.

   A página de topologia de recurso ou grupo de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Selecione o backup de dados da tabela e clique em  .
6. Na página Localização, execute as seguintes ações:

Para este campo…	Faça isso…
Servidor clone	Escolha um host no qual o clone deve ser criado.
Instância do clone de destino	Insira o ID da instância do clone do Db2 de destino a ser clonado dos backups existentes. Isso é aplicável somente ao recurso do tipo de armazenamento ANF.
Nome do clone de destino	Digite o nome do clone. Isso é aplicável somente ao recurso de banco de dados Db2.
Endereço IP de exportação NFS	Insira os endereços IP ou os nomes de host nos quais os volumes clonados serão exportados. Isso é aplicável somente ao recurso do tipo de armazenamento NFS.
Pool de Capacidade Máxima Taxa de Transferência (MiB/s)	Insira a taxa de transferência máxima de um pool de capacidade.

7. Na página Scripts, execute as seguintes etapas:

   Os scripts são executados no host do plug-in.

   a. Insira os comandos para pré-clonagem ou pós-clonagem que devem ser executados antes ou depois da operação de clonagem, respectivamente.

- Comando pré-clone: exclui bancos de dados existentes com o mesmo nome
- Comando post clone: verifica um banco de dados ou inicia um banco de dados.

b. Digite o comando mount para montar um sistema de arquivos em um host.

Comando de montagem para um volume ou qtree em uma máquina Linux:

Exemplo para NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail.

9. Revise o resumo e clique em **Concluir**.
10. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Depois que você terminar

Após clonar os recursos do Db2 descobertos automaticamente, o recurso clonado é marcado como recurso manual. Clique em **Atualizar recursos** para recuperar o recurso Db2 clonado. Quando você exclui o clone, o armazenamento e o host também são limpos.

Se você não atualizar os recursos após a operação de clonagem e tentar excluir o clone, o armazenamento e o host não serão limpos. Você deve excluir as entradas manualmente no fstab.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Liste os backups que podem ser clonados usando o cmdlet Get-SmBackup ou Get-SmResourceGroup.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                    BackupTime   BackupType
--------   ----------                    ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

   Este exemplo exibe informações sobre um grupo de recursos especificado, seus recursos e políticas

associadas:

```
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. Inicie uma operação de clonagem de um backup existente usando o cmdlet New-SmClone.

   Este exemplo cria um clone de um backup especificado com todos os logs:

```
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
```

   Este exemplo cria um clone para uma instância especificada do Microsoft SQL Server:

```
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. Visualize o status do trabalho de clonagem usando o cmdlet Get-SmCloneReport.

   Este exemplo exibe um relatório de clone para o ID do trabalho especificado:

```
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}
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitorar operações de clone do IBM Db2

Você pode monitorar o progresso das operações de clonagem do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique  para filtrar a lista de modo que somente operações de clonagem sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione o trabalho de clonagem e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página Detalhes do trabalho, clique em **Exibir registros**.

Dividir um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido se torna independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clone em um clone intermediário.

  Por exemplo, depois de criar o clone1 a partir de um backup de banco de dados, você pode criar um backup do clone1 e então clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e você não pode executar a operação de divisão de clone no clone1. No entanto, você pode executar a operação de divisão de clone no clone2.

  Após dividir o clone2, você pode executar a operação de divisão do clone no clone1 porque o clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e os trabalhos de clonagem do clone são excluídos.
- Para obter informações sobre as operações de divisão de volume do FlexClone , consulte "Dividir um volume FlexClone de seu volume pai" .
- Certifique-se de que o volume ou agregado no sistema de armazenamento esteja online.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página **Recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicações de banco de dados	Selecione **Banco de dados** na lista Exibir.
Para sistemas de arquivos	Selecione **Caminho** na lista Exibir.

3. Selecione o recurso apropriado na lista.

   A página de topologia de recursos é exibida.

4. Na exibição **Gerenciar cópias**, selecione o recurso clonado (por exemplo, o banco de dados ou LUN) e

clique em *  *.

5. Revise o tamanho estimado do clone que será dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

   A operação de divisão do clone para de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clone e, em seguida, tentar novamente a operação de divisão de clone.

   Se você quiser um tempo de pesquisa maior ou menor para verificar se o clone está dividido ou não, você pode alterar o valor do parâmetro *CloneSplitStatusCheckPollTime* no arquivo *SMCoreServiceHost.exe.config* para definir o intervalo de tempo para o SMCore pesquisar o status da operação de divisão do clone. O valor está em milissegundos e o valor padrão é 5 minutos.

   Por exemplo:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   A operação de início da divisão do clone falha se um backup, uma restauração ou outra divisão do clone estiver em andamento. Você deve reiniciar a operação de divisão do clone somente após a conclusão das operações em execução.

Informações relacionadas

"O clone ou a verificação do SnapCenter falham com o agregado inexistente"

Excluir ou dividir clones do banco de dados IBM Db2 após atualizar o SnapCenter

Após atualizar para o SnapCenter 4.3, você não verá mais os clones. Você pode excluir o clone ou dividir os clones na página Topologia do recurso a partir do qual os clones foram criados.

Sobre esta tarefa

Se você quiser localizar a pegada de armazenamento dos clones ocultos, execute o seguinte comando: `Get-SmClone -ListStorageFootprint`

Passos

1. Exclua os backups dos recursos clonados usando o cmdlet remove-smbackup.
2. Exclua o grupo de recursos dos recursos clonados usando o cmdlet remove-smresourcegroup.
3. Remova a proteção do recurso clonado usando o cmdlet remove-smprotectresource.
4. Selecione o recurso pai na página Recursos.

   A página de topologia de recursos é exibida.

5. Na exibição Gerenciar cópias, selecione os clones dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
6. Selecione os clones e clique em  para excluir clones ou clicar  para dividir os clones.
7. Clique em **OK**.

Proteger PostgreSQL

Plug-in SnapCenter para PostgreSQL

Visão geral do plug-in SnapCenter para PostgreSQL

O plug-in SnapCenter para cluster PostgreSQL é um componente do lado do host do software NetApp SnapCenter software que permite o gerenciamento de proteção de dados com reconhecimento de aplicativo de clusters PostgreSQL. O plug-in para cluster PostgreSQL automatiza o backup, a restauração e a clonagem de clusters PostgreSQL no seu ambiente SnapCenter .

O SnapCenter oferece suporte a configurações de cluster único e multicluster do PostgreSQL. Você pode usar o Plug-in para Clusters PostgreSQL em ambientes Linux e Windows. Em ambientes Windows, o PostgreSQL será suportado como recurso manual.

Quando o cluster Plug-in para PostgreSQL estiver instalado, você poderá usar o SnapCenter com a tecnologia NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume. Você também pode usar o plug-in com a tecnologia NetApp SnapVault para executar a replicação de backup de disco para disco para conformidade com os padrões.

O plug-in SnapCenter para PostgreSQL oferece suporte a NFS e SAN em layouts de armazenamento de arquivos ONTAP e Azure NetApp .

O layout de armazenamento virtual VMDK, vVol e RDM é suportado.

O que você pode fazer usando o plug-in SnapCenter para PostgreSQL

Ao instalar o plug-in para cluster PostgreSQL em seu ambiente, você pode usar o SnapCenter para fazer backup, restaurar e clonar clusters PostgreSQL e seus recursos. Você também pode executar tarefas de suporte a essas operações.

- Adicionar clusters.
- Crie backups.
- Restaurar a partir de backups.
- Clonar backups.
- Agende operações de backup.
- Monitore operações de backup, restauração e clonagem.
- Visualize relatórios de operações de backup, restauração e clonagem.

Recursos do plug-in SnapCenter para PostgreSQL

O SnapCenter integra-se ao aplicativo plug-in e às tecnologias NetApp no sistema de armazenamento. Para trabalhar com o Plug-in para o Cluster PostgreSQL, use a interface gráfica do usuário do SnapCenter .

- **Interface gráfica de usuário unificada**

A interface do SnapCenter fornece padronização e consistência entre plug-ins e ambientes. A interface do SnapCenter permite que você conclua operações consistentes de backup, restauração e clonagem em plug-ins, use relatórios centralizados, use visualizações de painel rápidas, configure o controle de acesso baseado em função (RBAC) e monitore trabalhos em todos os plug-ins.

- **Administração central automatizada**

  Você pode agendar operações de backup, configurar retenção de backup baseada em políticas e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- *Tecnologia de cópia instantânea não disruptiva da NetApp *

  O SnapCenter usa a tecnologia de snapshot da NetApp com o plug-in para cluster PostgreSQL para fazer backup de recursos.

Usar o Plug-in para PostgreSQL também oferece os seguintes benefícios:

- Suporte para fluxos de trabalho de backup, restauração e clonagem
- Segurança com suporte RBAC e delegação centralizada de funções

  Você também pode definir as credenciais para que os usuários autorizados do SnapCenter tenham permissões no nível do aplicativo.

- Criação de cópias de recursos com eficiência de espaço e em um determinado momento para testes ou extração de dados usando a tecnologia NetApp FlexClone

  Uma licença FlexClone é necessária no sistema de armazenamento onde você deseja criar o clone.

- Suporte para o recurso de instantâneo do grupo de consistência (CG) do ONTAP como parte da criação de backups.
- Capacidade de executar vários backups simultaneamente em vários hosts de recursos

  Em uma única operação, os snapshots são consolidados quando recursos em um único host compartilham o mesmo volume.

- Capacidade de criar snapshots usando comandos externos.
- Suporte para Linux LVM no sistema de arquivos XFS.

Tipos de armazenamento suportados pelo SnapCenter Plug-in para PostgreSQL

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e virtuais (VMs). Você deve verificar o suporte para seu tipo de armazenamento antes de instalar o SnapCenter Plug-in para PostgreSQL.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados por FC • LUNs conectados por iSCSI • Volumes conectados ao NFS

Máquina	Tipo de armazenamento
VMware ESXi	• LUNs RDM conectados por um FC ou iSCSI ESXi HBAA varredura de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluída porque o SnapCenter verifica todos os adaptadores de barramento de host presentes no host. Você pode editar o arquivo **LinuxConfig.pm** localizado em */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* para definir o valor do parâmetro **SCSI_HOSTS_OPTIMIZED_RESCAN** como 1 para verificar novamente apenas os HBAs listados em HBA_DRIVER_NAMES. • LUNs iSCSI conectados diretamente ao sistema convidado pelo iniciador iSCSI • VMDKs em armazenamentos de dados NFS • VMDKs no VMFS • Volumes NFS conectados diretamente ao sistema convidado • Armazenamentos de dados vVol em NFS e SAN O armazenamento de dados vVol só pode ser provisionado com o ONTAP Tools para VMware vSphere.

Privilégios ONTAP mínimos necessários para o plug-in PostgreSQL

Os privilégios mínimos do ONTAP necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos de acesso total: privilégios mínimos necessários para ONTAP 9.12.1 e posterior
  - evento generate-autosupport-log
  - histórico de trabalho mostrar
  - parada de trabalho
  - lua
  - lun criar
  - lun criar
  - lun criar
  - lun delete
  - lun igroup adicionar
  - lun igroup criar

- lun igroup excluir
- renomear lun igroup
- renomear lun igroup
- show do lun igroup
- mapeamento lun add-reporting-nodes
- criação de mapeamento lun
- exclusão de mapeamento lun
- mapeamento lun remove-reporting-nodes
- show de mapeamento lunar
- lun modificar
- volume de entrada lun
- lua offline
- lua online
- lun persistente-reserva clara
- redimensionamento de lun
- série lun
- show de lua
- política de adição de regra do snapmirror
- regra de modificação de política do snapmirror
- política de remoção do snapmirror
- política do snapmirror mostrar
- restauração do snapmirror
- show de espelhos instantâneos
- histórico de exibição do snapmirror
- atualização do snapmirror
- atualização do snapmirror-ls-set
- lista-destinos do snapmirror
- versão
- criação de clone de volume
- show de clones de volume
- volume clone split start
- volume clone divisão parada
- volume criar
- destruição de volume
- clone de arquivo de volume criar
- arquivo de volume mostrar-uso-do-disco
- volume offline

    - volume on-line
    - modificação de volume
    - volume qtree criar
    - volume qtree delete
    - volume qtree modificar
    - volume qtree mostrar
    - restrição de volume
    - show de volume
    - criação de instantâneo de volume
    - exclusão de instantâneo de volume
    - modificação de instantâneo de volume
    - instantâneo de volume modificar-tempo-de-expiração-do-snaplock
    - renomeação de instantâneo de volume
    - restauração de instantâneo de volume
    - arquivo de restauração de instantâneo de volume
    - exibição de instantâneo de volume
    - desmontagem de volume
    - cifs do vserver
    - vserver cifs compartilhar criar
    - vserver cifs compartilhar excluir
    - vserver cifs shadowcopy mostrar
    - vserver cifs compartilhar mostrar
    - vserver cifs mostrar
    - política de exportação do vserver
    - criação de política de exportação do vserver
    - exclusão da política de exportação do vserver
    - criação de regra de política de exportação do vserver
    - mostrar regra de política de exportação do vserver
    - mostrar política de exportação do vserver
    - vserver iscsi
    - mostrar conexão iscsi do vserver
    - vserver mostrar
- Comandos somente leitura: privilégios mínimos necessários para ONTAP 8.3.0 e posterior
    - interface de rede
    - exibição de interface de rede
    - vserver

Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para PostgreSQL

Você pode usar um plug-in SnapCenter com a tecnologia ONTAP SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia ONTAP SnapVault para executar replicação de backup de disco para disco para conformidade com padrões e outros propósitos relacionados à governança. Antes de executar essas tarefas, você deve configurar um relacionamento de proteção de dados entre os volumes de origem e destino e inicializar o relacionamento.

O SnapCenter executa as atualizações no SnapMirror e no SnapVault após concluir a operação Snapshot. As atualizações do SnapMirror e do SnapVault são executadas como parte do trabalho do SnapCenter ; não crie uma programação ONTAP separada.

Se você estiver acessando o SnapCenter a partir de um produto NetApp SnapManager e estiver satisfeito com os relacionamentos de proteção de dados configurados, pode pular esta seção.

Um relacionamento de proteção de dados replica dados do armazenamento primário (o volume de origem) para o armazenamento secundário (o volume de destino). Quando você inicializa o relacionamento, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não oferece suporte a relacionamentos em cascata entre volumes SnapMirror e SnapVault (**Primário** > **Espelho** > **Cofre**). Você deve usar relacionamentos fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis em termos de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis em termos de versão e como configurá-los, consulte "Documentação do ONTAP" .

Estratégia de backup para PostgreSQL

Definir uma estratégia de backup para PostgreSQL

Definir uma estratégia de backup antes de criar suas tarefas de backup ajuda você a ter os backups necessários para restaurar ou clonar seus recursos com sucesso. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (RTO) e objetivo de ponto de recuperação (RPO) determinam em grande parte sua estratégia de backup.

Sobre esta tarefa

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. RTO é o tempo em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. SLA, RTO e RPO contribuem para a estratégia de proteção de dados.

Passos

1. Determine quando você deve fazer backup dos seus recursos.
2. Decida quantos trabalhos de backup você precisa.
3. Decida como nomear seus backups.

4. Decida se você deseja criar uma política baseada em cópia de instantâneo para fazer backup de instantâneos consistentes com o aplicativo do cluster.
5. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção de longo prazo.
6. Determine o período de retenção dos snapshots no sistema de armazenamento de origem e no destino do SnapMirror .
7. Determine se você deseja executar algum comando antes ou depois da operação de backup e forneça uma prescrição ou pós-escrito.

Descoberta automática de recursos no host Linux

Os recursos são clusters e instâncias do PostgreSQL no host Linux que são gerenciados pelo SnapCenter. Após instalar o plug-in SnapCenter para PostgreSQL, os clusters PostgreSQL de todas as instâncias naquele host Linux são descobertos automaticamente e exibidos na página Recursos.

Tipo de backups suportados

O tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter oferece suporte ao tipo de backup baseado em cópia de snapshot para clusters PostgreSQL.

Backup baseado em cópia instantânea

Os backups baseados em cópias de instantâneo aproveitam a tecnologia de instantâneo da NetApp para criar cópias on-line somente leitura dos volumes nos quais os clusters PostgreSQL residem.

Como o plug-in SnapCenter para PostgreSQL usa instantâneos de grupo de consistência

Você pode usar o plug-in para criar instantâneos de grupos de consistência para grupos de recursos. Um grupo de consistência é um contêiner que pode abrigar vários volumes para que você possa gerenciá-los como uma única entidade. Um grupo de consistência é composto por instantâneos simultâneos de vários volumes, fornecendo cópias consistentes de um grupo de volumes.

Você também pode especificar o tempo de espera para que o controlador de armazenamento agrupe snapshots de forma consistente. As opções de tempo de espera disponíveis são **Urgente**, **Médio** e **Relaxado**. Você também pode habilitar ou desabilitar a sincronização do Write Anywhere File Layout (WAFL) durante a operação consistente de snapshot de grupo. A sincronização do WAFL melhora o desempenho de um instantâneo de grupo de consistência.

Como o SnapCenter gerencia a manutenção de backups de dados

O SnapCenter gerencia a manutenção de backups de dados nos níveis do sistema de armazenamento e do sistema de arquivos.

Os snapshots no armazenamento primário ou secundário e suas entradas correspondentes no catálogo PostgreSQL são excluídos com base nas configurações de retenção.

Considerações para determinar agendamentos de backup para PostgreSQL

O fator mais crítico na determinação de um cronograma de backup é a taxa de alteração do recurso. Você pode fazer backup de um recurso muito utilizado a cada hora, enquanto pode fazer backup de um recurso raramente utilizado uma vez por dia. Outros fatores incluem a importância do recurso para sua organização, seu acordo de nível de serviço (SLA) e seu objetivo de ponto de recuperação (RPO).

Os agendamentos de backup têm duas partes, conforme a seguir:

- Frequência de backup (com que frequência os backups devem ser realizados)

  A frequência de backup, também chamada de tipo de agendamento para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como horária, diária, semanal ou mensal.

- Agendamentos de backup (exatamente quando os backups devem ser executados)

  Os agendamentos de backup fazem parte de uma configuração de recurso ou grupo de recursos. Por exemplo, se você tiver um grupo de recursos com uma política configurada para backups semanais, poderá configurar o agendamento para fazer backup todas as quintas-feiras às 22h.

Número de trabalhos de backup necessários para PostgreSQL

Os fatores que determinam o número de tarefas de backup necessárias incluem o tamanho do recurso, o número de volumes usados, a taxa de alteração do recurso e seu Contrato de Nível de Serviço (SLA).

Convenções de nomenclatura de backup para clusters do Plug-in para PostgreSQL

Você pode usar a convenção de nomenclatura padrão do Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um registro de data e hora aos nomes de instantâneos que ajuda a identificar quando as cópias foram criadas.

O Snapshot usa a seguinte convenção de nomenclatura padrão:

```
resourcegroupname_hostname_timestamp
```

Você deve nomear seus grupos de recursos de backup logicamente, como no exemplo a seguir:

```
dts1_mach1x88_03-12-2015_23.17.26
```

Neste exemplo, os elementos de sintaxe têm os seguintes significados:

- *dts1* é o nome do grupo de recursos.
- *mach1x88* é o nome do host.
- *03-12-2015_23.17.26* é a data e o registro de data e hora.

Como alternativa, você pode especificar o formato do nome do Snapshot ao proteger recursos ou grupos de recursos selecionando **Usar formato de nome personalizado para cópia do Snapshot**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do registro de data e hora é adicionado ao nome do Snapshot.

Estratégia de restauração e recuperação para PostgreSQL

Definir uma estratégia de restauração e recuperação para recursos do PostgreSQL

Você deve definir uma estratégia antes de restaurar e recuperar seu cluster para que possa executar operações de restauração e recuperação com sucesso.

Somente a recuperação manual do cluster é suportada.

Passos

1. Determinar as estratégias de restauração suportadas para recursos PostgreSQL adicionados manualmente
2. Determinar as estratégias de restauração suportadas para clusters PostgreSQL descobertos automaticamente
3. Decida o tipo de operações de recuperação que você deseja executar.

Tipos de estratégias de restauração suportadas para recursos PostgreSQL adicionados manualmente

Você deve definir uma estratégia antes de poder executar com sucesso operações de restauração usando o SnapCenter.

Não é possível recuperar recursos do PostgreSQL adicionados manualmente.

Restauração completa de recursos

- Restaura todos os volumes, qtrees e LUNs de um recurso

Se o recurso contiver volumes ou qtrees, os instantâneos tirados após o instantâneo selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

OBSERVAÇÃO: O plug-in para PostgreSQL cria um backup_label e um tablespace_map na pasta */<OS_temp_folder>/postgresql_sc_recovery*<Restore_JobId>/_ para ajudar na recuperação manual.

Tipo de estratégia de restauração suportada para PostgreSQL descoberto automaticamente

Você deve definir uma estratégia antes de poder executar com sucesso operações de restauração usando o SnapCenter.

A restauração completa de recursos é a estratégia de restauração suportada por clusters PostgreSQL descobertos automaticamente. Isso restaura todos os volumes, qtrees e LUNs de um recurso.

Tipos de operações de restauração para PostgreSQL descoberto automaticamente

O plug-in SnapCenter para PostgreSQL oferece suporte a Single File SnapRestore e tipos de restauração de conexão e cópia para clusters PostgreSQL descobertos automaticamente.

O Single File SnapRestore é executado em ambientes NFS para os seguintes cenários:

- Se apenas a opção **Recurso Completo** for selecionada
- Quando o backup selecionado for de um local secundário do SnapMirror ou SnapVault e a opção **Recurso Completo** for selecionada

O Single File SnapRestore é executado em ambientes SAN para os seguintes cenários:

- Se apenas a opção **Recurso Completo** for selecionada
- Quando o backup é selecionado de um local secundário do SnapMirror ou SnapVault e a opção **Recurso Completo** é selecionada

Tipos de operações de recuperação suportadas para clusters PostgreSQL

O SnapCenter permite que você execute diferentes tipos de operações de recuperação para clusters PostgreSQL.

- Recuperar o cluster até o estado mais recente
- Recuperar o cluster até um ponto específico no tempo

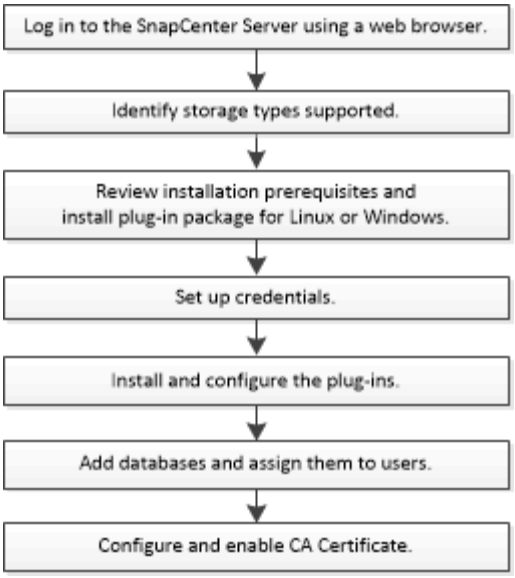
  Você deve especificar a data e a hora da recuperação.

O SnapCenter também oferece a opção Sem recuperação para clusters PostgreSQL.

Prepare-se para instalar o plug-in SnapCenter para PostgreSQL

Fluxo de trabalho de instalação do plug-in SnapCenter para PostgreSQL

Você deve instalar e configurar o SnapCenter Plug-in para PostgreSQL se quiser proteger clusters PostgreSQL.



Pré-requisitos para adicionar hosts e instalar o plug-in SnapCenter para PostgreSQL

Antes de adicionar um host e instalar os pacotes de plug-in, você deve concluir todos os requisitos. O plug-in SnapCenter para PostgreSQL está disponível em ambientes Windows e Linux.

- Você deve ter instalado o Java 11 no seu host.

  O IBM Java não é suportado em hosts Windows e Linux.

- No Windows, o Plug-in Creator Service deve ser executado usando o usuário do Windows “LocalSystem”, que é o comportamento padrão quando o Plug-in para PostgreSQL é instalado como administrador de domínio.
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host. O plug-in SnapCenter para Microsoft Windows será implantado por padrão com o plug-in PostgreSQL em hosts Windows.
- O SnapCenter Server deve ter acesso à porta 8145 ou personalizada do host Plug-in para PostgreSQL.

Hosts do Windows

- Você deve ter um usuário de domínio com privilégios de administrador local e permissões de login local no host remoto.
- Ao instalar o Plug-in para PostgreSQL em um host Windows, o SnapCenter Plug-in para Microsoft Windows é instalado automaticamente.
- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 no seu host Windows.

  "Baixe JAVA para todos os sistemas operacionais"

  "Ferramenta de Matriz de Interoperabilidade da NetApp"

Hosts Linux

- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 no seu host Linux.

  "Baixe JAVA para todos os sistemas operacionais"

  "Ferramenta de Matriz de Interoperabilidade da NetApp"

- Para clusters PostgreSQL em execução em um host Linux, ao instalar o Plug-in para PostgreSQL, o SnapCenter Plug-in para UNIX é instalado automaticamente.
- Você deve ter **bash** como o shell padrão para instalação de plug-ins.

Comandos suplementares

Para executar um comando suplementar no SnapCenter Plug-in para PostgreSQL, você deve incluí-lo no arquivo *allowed_commands.config*.

- Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Para permitir comandos suplementares no host do plug-in, abra o arquivo *allowed_commands.config* em um editor. Digite cada comando em uma linha separada e os comandos não diferenciam maiúsculas de minúsculas. Certifique-se de especificar o caminho totalmente qualificado e coloque-o entre aspas (") se ele contiver espaços.

Por exemplo:

comando: mount comando: umount comando: "C:\Arquivos de Programas\ NetApp\SnapCreator commands\sdcli.exe" comando: myscript.bat

Se o arquivo *allowed_commands.config* não estiver presente, os comandos ou a execução do script serão bloqueados e o fluxo de trabalho falhará com o seguinte erro:

"[/mnt/mount -a] execução não permitida. Autorize adicionando o comando no arquivo %s no host do plugin."

Se o comando ou script não estiver presente no *allowed_commands.config*, a execução do comando ou script será bloqueada e o fluxo de trabalho falhará com o seguinte erro:

"[/mnt/mount -a] execução não permitida. Autorize adicionando o comando no arquivo %s no host do plugin."

Você não deve usar uma entrada curinga (*) para permitir todos os comandos.

Configurar privilégios sudo para usuários não root para host Linux

O SnapCenter permite que um usuário não root instale o pacote de plug-ins do SnapCenter para Linux e inicie o processo de plug-in. Os processos do plug-in serão executados como um usuário não root efetivo. Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.

- Se a umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro dela tenham permissão de 555. Caso contrário, a instalação do plug-in poderá falhar.
- Para o usuário não root, certifique-se de que o nome do usuário não root e o nome do grupo do usuário sejam os mesmos.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos do código de autenticação de mensagens: MACs hmac-sha2-256 e MACs hmac-sha2-512.

  Reinicie o serviço sshd após atualizar o arquivo de configuração.

  Exemplo:

```
#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
```

Sobre esta tarefa

Você deve configurar privilégios sudo para que o usuário não root forneça acesso aos seguintes caminhos:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /localização_personalizada/ NetApp/snapcenter/spl/instalação/plugins/desinstalação
- /localização_personalizada/ NetApp/snapcenter/spl/bin/spl

Passos

1. Efetue login no host Linux no qual você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
2. Adicione as seguintes linhas ao arquivo /etc/sudoers usando o utilitário visudo Linux.

```
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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

LINUX_USER é o nome do usuário não root que você criou.

Você pode obter o *checksum_value* do arquivo **sc_unix_plugins_checksum.txt**, localizado em:

- _C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _ se o SnapCenter Server estiver instalado no host Windows.
- _/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ se o SnapCenter Server estiver instalado no host Linux.

O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows

Antes de instalar o pacote de plug-ins do SnapCenter para Windows, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas Operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB

Item	Requisitos
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	5 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell Core 7.4.2 Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux

Antes de instalar o pacote de plug-ins SnapCenter para Linux, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas operacionais	• Red Hat Enterprise Linux • Servidor SUSE Linux Enterprise (SLES) Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB

Item	Requisitos
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	2 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	Java 11 Oracle Java e OpenJDK Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em /var/opt/snapcenter/spl/etc/spl.properties esteja definida para a versão correta do JAVA e o caminho correto. Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Configurar credenciais para o plug-in SnapCenter para PostgreSQL

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter . Você deve criar credenciais para instalar plug-ins do SnapCenter e credenciais adicionais para executar operações de proteção de dados em clusters ou sistemas de arquivos do Windows.

Sobre esta tarefa

- Hosts Linux

  Você deve configurar credenciais para instalar plug-ins em hosts Linux.

  Você deve configurar as credenciais para o usuário root ou para um usuário não root que tenha privilégios sudo para instalar e iniciar o processo do plug-in.

  Melhores práticas: embora você tenha permissão para criar credenciais para o Linux após implantar hosts e instalar plug-ins, a melhor prática é criar credenciais depois de adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

  Você deve configurar as credenciais do Windows antes de instalar plug-ins.

Você deve configurar as credenciais com privilégios de administrador, incluindo direitos de administrador no host remoto.

Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver privilégios de administrador completos, será necessário atribuir pelo menos os privilégios de grupo de recursos e backup ao nome de usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.
4. Na página Credencial, especifique as informações necessárias para configurar as credenciais:

Para este campo…	Faça isso…
Nome da credencial	Digite um nome para as credenciais.

Para este campo…	Faça isso…
Nome de usuário	Digite o nome de usuário e a senha que serão usados para autenticação. • Administrador de domínio ou qualquer membro do grupo de administradores Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS\Nome do Usuário* ◦ *FQDN do domínio\Nome do usuário* • Administrador local (somente para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é: *UserName* Não use aspas duplas (") ou acento grave (`) nas senhas. Você não deve usar os símbolos de menor que (<) e exclamação (!) juntos em senhas. Por exemplo, menor que <! 10, menor que 10 <!, acento grave `12.
Senha	Digite a senha usada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que você deseja usar.
Use privilégios sudo	Marque a caixa de seleção **Usar privilégios sudo** se estiver criando credenciais para um usuário não root. Aplicável somente a usuários do Linux.

5. Clique em **OK**.

Depois de concluir a configuração das credenciais, talvez você queira atribuir a manutenção de credenciais a um usuário ou grupo de usuários na página Usuário e Acesso.

Configurar o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite que você crie uma Conta de Serviço Gerenciada de grupo (gMSA) que fornece gerenciamento automatizado de senhas de contas de serviço a partir de uma conta de domínio gerenciada.

Antes de começar

- Você deve ter um controlador de domínio do Windows Server 2016 ou posterior.
- Você deve ter um host Windows Server 2016 ou posterior, que seja membro do domínio.

Passos

1. Crie uma chave raiz do KDS para gerar senhas exclusivas para cada objeto no seu gMSA.
2. Para cada domínio, execute o seguinte comando no controlador de domínio do Windows: Add-KDSRootKey -EffectiveImmediately
3. Crie e configure seu gMSA:
   a. Crie uma conta de grupo de usuários no seguinte formato:

```
 domainName\accountName$
.. Adicione objetos de computador ao grupo.
.. Use o grupo de usuários que você acabou de criar para criar o
gMSA.
```

   Por exemplo,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correr `Get-ADServiceAccount` comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Habilite o módulo do Active Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando no PowerShell:

```
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. Reinicie seu host.

b. Instale o gMSA no seu host executando o seguinte comando no prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua privilégios administrativos ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no SnapCenter Server.

   O SnapCenter Server instalará os plug-ins selecionados no host e o gMSA especificado será usado como a conta de logon de serviço durante a instalação do plug-in.

Instalar o plug-in SnapCenter para PostgreSQL

Adicionar hosts e instalar pacotes de plug-ins em hosts remotos

Você deve usar a página Adicionar Host do SnapCenter para adicionar hosts e, em seguida, instalar os pacotes de plug-ins. Os plug-ins são instalados automaticamente nos hosts remotos. Você pode adicionar o host e instalar pacotes de plug-in para um host individual.

Antes de começar

- Se o sistema operacional do host do SnapCenter Server for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deverá executar o seguinte:
  - Atualize para o Windows Server 2019 (versão do sistema operacional 17763.5936) ou posterior
  - Atualize para o Windows Server 2022 (versão do sistema operacional 20348.2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada

ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.

- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- A documentação de administração contém informações sobre o gerenciamento de hosts.
- Se estiver usando uma conta de serviço gerenciada em grupo (gMSA), você deverá configurar a gMSA com privilégios administrativos.

  "Configurar conta de serviço gerenciada de grupo no Windows Server 2016 ou posterior para PostgreSQL"

Sobre esta tarefa

- Não é possível adicionar um SnapCenter Server como um host de plug-in a outro SnapCenter Server.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Clique em **Adicionar**.
4. Na página Hosts, execute as seguintes ações:

Para este campo…	Faça isso…
Tipo de host	Selecione o tipo de host: • Windows • Linux O plug-in para PostgreSQL é instalado no host do cliente PostgreSQL, e esse host pode estar em um sistema Windows ou Linux.
Nome do host	Digite o nome do host de comunicação. Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o FQDN.

Para este campo…	Faça isso…
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais. Você pode visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial fornecida. O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar Host.

5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a serem instalados.

   Ao usar a API REST para instalar o Plug-in para PostgreSQL, você deve passar a versão como 3.0. Por exemplo, PostgreSQL:3.0

6. (Opcional) Clique em **Mais opções**.

Para este campo…	Faça isso…
Porta	Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.
Caminho de instalação	O plug-in para PostgreSQL é instalado no host do cliente PostgreSQL, e esse host pode estar em um sistema Windows ou Linux. • Para o pacote de plug-ins SnapCenter para Windows, o caminho padrão é C:\Arquivos de Programas\ NetApp\ SnapCenter. Opcionalmente, você pode personalizar o caminho. • Para o pacote de plug-ins SnapCenter para Linux, o caminho padrão é /opt/ NetApp/snapcenter. Opcionalmente, você pode personalizar o caminho.

Para este campo…	Faça isso…
Ignorar verificações de pré-instalação	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.
Adicionar todos os hosts no cluster	Marque esta caixa de seleção para adicionar todos os nós do cluster.
Use a conta de serviço gerenciada em grupo (gMSA) para executar os serviços do plug-in	Para o host Windows, marque esta caixa de seleção se desejar usar a Conta de Serviço Gerenciada em Grupo (gMSA) para executar os serviços do plug-in. Forneça o nome do gMSA no seguinte formato: domainName\accountName$. O gMSA será usado como uma conta de serviço de logon somente para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

   Se você não tiver marcado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se ele atende aos requisitos para a instalação do plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão do .NET, a localização (para plug-ins do Windows) e a versão do Java (para plug-ins do Linux) são validados em relação aos requisitos mínimos. Se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas serão exibidas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em C:\Arquivos de Programas\ NetApp\ SnapCenter WebApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, deverá atualizar o arquivo em ambos os nós.

8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirmar e Enviar**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós do cluster.

   A verificação de impressão digital é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitore o progresso da instalação.
   - Para o plug-in do Windows, os logs de instalação e atualização estão localizados em: *C:\Windows\ SnapCenter plugin\Install*<JOBID>_
   - Para o plug-in Linux, os logs de instalação estão localizados em: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log_ e os logs de

atualização estão localizados em: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log_

Instalar pacotes de plug-in SnapCenter para Linux ou Windows em vários hosts remotos usando cmdlets

Você pode instalar os pacotes de plug-in do SnapCenter para Linux ou Windows em vários hosts simultaneamente usando o cmdlet Install-SmHostPackage do PowerShell.

Antes de começar

Você deve ter efetuado login no SnapCenter como um usuário de domínio com direitos de administrador local em cada host no qual deseja instalar o pacote de plug-in.

Passos

1. Inicie o PowerShell.
2. No host do SnapCenter Server, estabeleça uma sessão usando o cmdlet Open-SmConnection e insira suas credenciais.
3. Instale o plug-in em vários hosts usando o cmdlet Install-SmHostPackage e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

   Você pode usar a opção -skipprecheck quando tiver instalado os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

4. Insira suas credenciais para instalação remota.

Instale o plug-in SnapCenter para PostgreSQL em hosts Linux usando a interface de linha de comando

Você deve instalar o plug-in SnapCenter para cluster PostgreSQL usando a interface de usuário (IU) do SnapCenter . Se o seu ambiente não permitir a instalação remota do plug-in pela interface do usuário do SnapCenter , você poderá instalar o cluster do Plug-in para PostgreSQL no modo de console ou no modo silencioso usando a interface de linha de comando (CLI).

Antes de começar

- Você deve instalar o cluster Plug-in para PostgreSQL em cada host Linux onde o cliente PostgreSQL reside.
- O host Linux no qual você está instalando o plug-in SnapCenter para cluster PostgreSQL deve atender aos requisitos de software, cluster e sistema operacional dependentes.

  A Ferramenta de Matriz de Interoperabilidade (IMT) contém as informações mais recentes sobre as configurações suportadas.

  "Ferramenta de Matriz de Interoperabilidade da NetApp"

- O plug-in SnapCenter para cluster PostgreSQL faz parte do pacote de plug-ins SnapCenter para Linux. Antes de instalar o SnapCenter Plug-ins Package para Linux, você já deve ter instalado o SnapCenter em um host Windows.

Passos

1. Copie o arquivo de instalação do pacote de plug-ins do SnapCenter para Linux (snapcenter_linux_host_plugin.bin) de C:\ProgramData\ NetApp\ SnapCenter\Package Repository para o host onde você deseja instalar o plug-in para PostgreSQL.

   Você pode acessar esse caminho a partir do host onde o SnapCenter Server está instalado.

2. No prompt de comando, navegue até o diretório onde você copiou o arquivo de instalação.
3. Instale o plug-in: `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 especifica a porta de comunicação HTTPS do SMCore.
   - -DSERVER_IP especifica o endereço IP do SnapCenter Server.
   - -DSERVER_HTTPS_PORT especifica a porta HTTPS do SnapCenter Server.
   - -DUSER_INSTALL_DIR especifica o diretório onde você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
   - DINSTALL_LOG_NAME especifica o nome do arquivo de log.

   ```
   /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. Edite o arquivo /<diretório de instalação>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties e adicione o parâmetro PLUGINS_ENABLED = PostgreSQL:3.0.
5. Adicione o host ao SnapCenter Server usando o cmdlet Add-Smhost e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitore o status da instalação do Plug-in para PostgreSQL

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos

- Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
   a. Clique em **Filtrar**.
   b. Opcional: especifique a data de início e término.
   c. No menu suspenso Tipo, selecione **Instalação de plug-in**.
   d. No menu suspenso Status, selecione o status da instalação.
   e. Clique em **Aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Configurar certificado CA

Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.

O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte "Como gerar um arquivo CSR de certificado CA" .

Se você possui o certificado CA para seu domínio (*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover**

Snapin.

2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Importar chave privada	Selecione a opção **Sim**, importe a chave privada e clique em **Avançar**.
Formato de arquivo de importação	Não faça alterações; clique em **Avançar**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

> O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: *.pfx, *.p12 e *.p7b).

7. Repita a Etapa 5 para a pasta “Pessoal”.

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

Passos

1. Execute o seguinte na GUI:
   a. Clique duas vezes no certificado.
   b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.
   c. Percorra a lista de campos e clique em **Impressão digital**.
   d. Copie os caracteres hexadecimais da caixa.
   e. Remova os espaços entre os números hexadecimais.

      Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
   a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o

certificado instalado recentemente pelo nome do assunto.

Get-ChildItem -Path Cert:\LocalMachine\My

b. Copie a impressão digital.

Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Por exemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Vincule o certificado recém-instalado aos serviços de plug-in do host
   do Windows, executando os seguintes comandos:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Por exemplo:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

Configurar o certificado CA para o serviço SnapCenter PostgreSQL Plug-ins no host Linux

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo 'keystore.jks', que está localizado em */opt/ NetApp/snapcenter/scc/etc* como seu

armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in a partir do arquivo de propriedades do agente do plug-in.

   É o valor correspondente à chave 'KEYSTORE_PASS'.

2. Alterar a senha do keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Altere a senha de todos os aliases de entradas de chave privada no
keystore para a mesma senha usada para o keystore:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

   Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

3. Reinicie o serviço após alterar a senha.

> A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Reinicie o serviço após configurar os certificados raiz ou
intermediários para conectar o trust-store.
```

> Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Adicione o certificado da CA com chave privada e pública.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Listar os certificados adicionados no keystore.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

   A senha padrão do keystore do plug-in é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Se o nome do alias no certificado da CA for longo e contiver espaços
   ou caracteres especiais ("*",","), altere o nome do alias para um nome
   simples:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configure o nome do alias do certificado CA no arquivo
   agent.properties.
   ```

   Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

Configurar lista de revogação de certificados (CRL) para plug-ins

Sobre esta tarefa

- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é ' opt/ NetApp/snapcenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties em relação à chave CRL_PATH.

   Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Configurar o certificado CA para o serviço SnapCenter PostgreSQL Plug-ins no host Windows

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo *keystore.jks*, que está localizado em *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* como seu armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in a partir do arquivo de propriedades do agente do plug-in.

   É o valor correspondente à chave *KEYSTORE_PASS*.

2. Alterar a senha do keystore:

   keytool -storepasswd -keystore keystore.jks

   > Se o comando "keytool" não for reconhecido no prompt de comando do Windows, substitua o comando keytool pelo seu caminho completo.

   C:\Arquivos de Programas\Java\<versão_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. Altere a senha de todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:

   keytool -keypasswd -alias "nome_do_alias_no_certificado" -keystore keystore.jks

   Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

4. Reinicie o serviço após alterar a senha.

   > A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

   keytool -list -v -keystore keystore.jks

4. Adicione um certificado raiz ou intermediário:

   keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Reinicie o serviço após configurar os certificados raiz ou intermediários para conectar o trust-store.

> Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo *keystore.jks*.
3. Listar os certificados adicionados no keystore:

   keytool -list -v -keystore keystore.jks

4. Adicione o certificado da CA com chave privada e pública.

   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS

5. Listar os certificados adicionados no keystore.

   keytool -list -v -keystore keystore.jks

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

   A senha padrão do keystore do plug-in é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

   keytool -keypasswd -alias "nome_do_alias_no_certificado_da_CA" -keystore keystore.jks

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

   Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

Configurar lista de revogação de certificados (CRL) para plug-ins SnapCenter

Sobre esta tarefa

- Para baixar o arquivo CRL mais recente para o certificado CA relacionado, consulte "Como atualizar o arquivo de lista de revogação de certificados no SnapCenter CA Certificate" .
- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é *'C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo *agent.properties* em relação à chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

   Os certificados recebidos serão verificados em relação a cada CRL.

Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *Get-SmCertificateSettings*.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- * * indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- * * indica que o certificado CA foi validado com sucesso.
- * * indica que o certificado CA não pôde ser validado.
- * * indica que as informações de conexão não puderam ser recuperadas.

Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Prepare-se para a proteção de dados

Pré-requisitos para usar o plug-in SnapCenter para PostgreSQL

Antes de usar o SnapCenter Plug-in para PostgreSQL, o administrador do SnapCenter deve instalar e configurar o SnapCenter Server e executar as tarefas de pré-requisito.

- Instalar e configurar o SnapCenter Server.
- Efetue login no SnapCenter Server.
- Configure o ambiente SnapCenter adicionando conexões do sistema de armazenamento e criando credenciais, se aplicável.
- Instale o Java 11 no seu host Linux ou Windows.

  Você deve definir o caminho Java na variável de caminho ambiental da máquina host.

- Configure o SnapMirror e o SnapVault se desejar replicação de backup.

Como recursos, grupos de recursos e políticas são usados para proteger o PostgreSQL

Antes de usar o SnapCenter, é útil entender os conceitos básicos relacionados às operações de backup, clonagem e restauração que você deseja executar. Você interage com recursos, grupos de recursos e políticas para diferentes operações.

- Os recursos geralmente são clusters PostgreSQL dos quais você faz backup ou clona com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host.

  Ao executar uma operação em um grupo de recursos, você executa essa operação nos recursos definidos no grupo de recursos de acordo com o cronograma especificado para o grupo de recursos.

  Você pode fazer backup sob demanda de um único recurso ou de um grupo de recursos. Você também pode executar backups agendados para recursos individuais e grupos de recursos.

- As políticas especificam a frequência de backup, replicação, scripts e outras características das operações de proteção de dados.

  Ao criar um grupo de recursos, você seleciona uma ou mais políticas para esse grupo. Você também pode selecionar uma política ao executar um backup sob demanda para um único recurso.

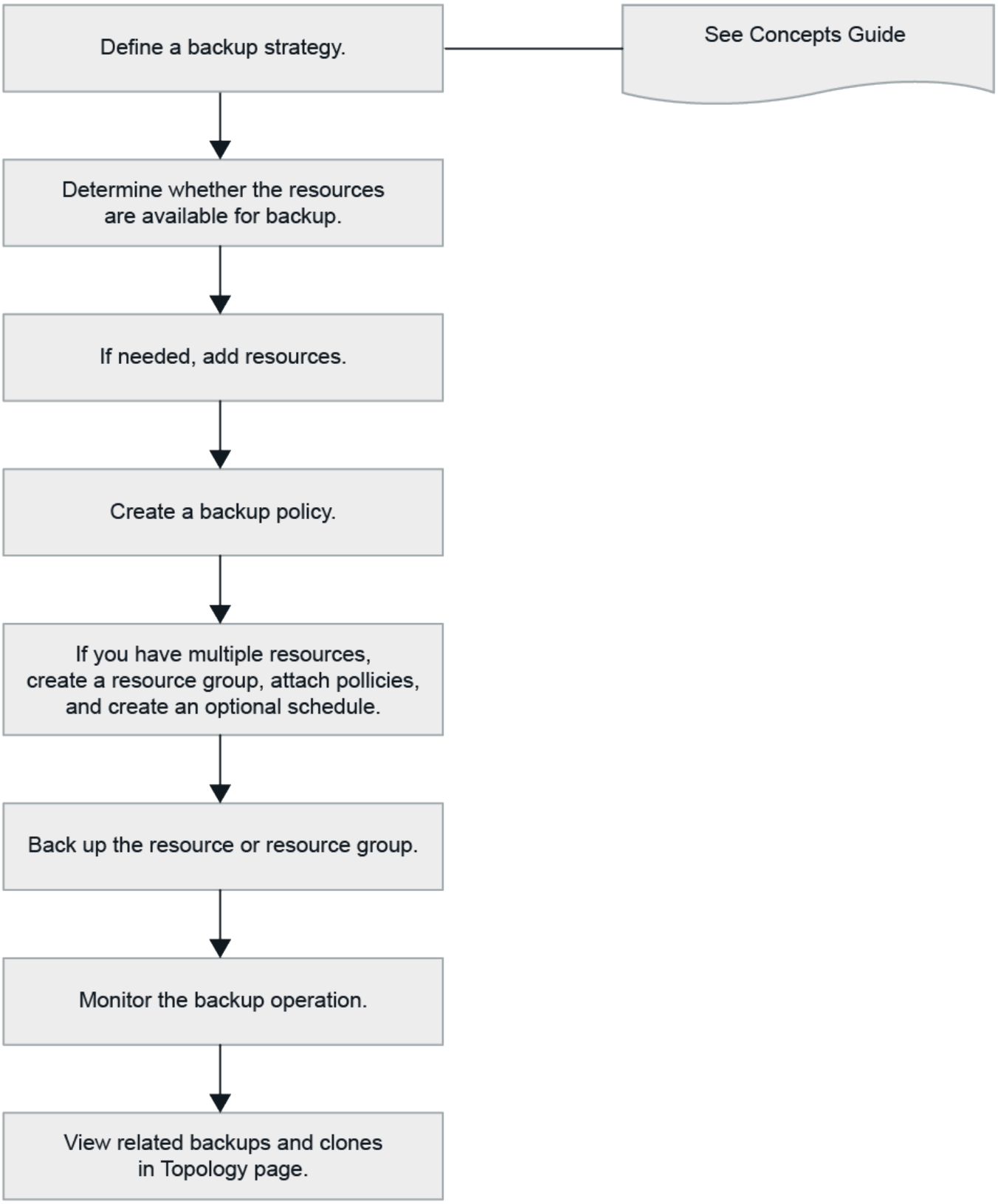
Pense em um grupo de recursos como algo que define o que você quer proteger e quando quer proteger em termos de dia e hora. Pense em uma política como a definição de como você deseja protegê-la. Se você estiver fazendo backup de todos os clusters, por exemplo, poderá criar um grupo de recursos que inclua todos os clusters no host. Você pode então anexar duas políticas ao grupo de recursos: uma política diária e uma política horária. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diariamente.

Fazer backup dos recursos do PostgreSQL

Fazer backup dos recursos do PostgreSQL

Você pode criar um backup de um recurso (cluster) ou grupo de recursos. O fluxo de trabalho de backup inclui planejamento, identificação de clusters para backup, gerenciamento de políticas de backup, criação de grupos de recursos e anexação de políticas, criação de backups e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de backup:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell. "Guia de referência do cmdlet do software SnapCenter" .

Descubra os clusters automaticamente

Os recursos são clusters PostgreSQL no host Linux que são gerenciados pelo SnapCenter. Você pode adicionar os recursos aos grupos de recursos para executar operações de proteção de dados depois de descobrir os clusters PostgreSQL que estão disponíveis.

Antes de começar

- Você já deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts e configurar as conexões do sistema de armazenamento.
- O plug-in SnapCenter para PostgreSQL não oferece suporte à descoberta automática de recursos que residem em ambientes virtuais RDM/VMDK.

Sobre esta tarefa

- Após instalar o plug-in, todos os clusters naquele host Linux são descobertos automaticamente e exibidos na página Recursos.
- Somente clusters são descobertos automaticamente.

Os recursos descobertos automaticamente não podem ser modificados ou excluídos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o Plug-in para PostgreSQL na lista.
2. Na página Recursos, selecione o tipo de recurso na lista Exibir.
3. (Opcional) Clique em * * e, em seguida, selecione o nome do host.

   Você pode então clicar em * * para fechar o painel de filtro.

4. Clique em **Atualizar recursos** para descobrir os recursos disponíveis no host.

   Os recursos são exibidos junto com informações como tipo de recurso, nome do host, grupos de recursos associados, tipo de backup, políticas e status geral.

   - Se o cluster estiver em um armazenamento NetApp e não estiver protegido, Não protegido será exibido na coluna Status geral.
   - Se o cluster estiver em um sistema de armazenamento NetApp e protegido, e se nenhuma operação de backup for realizada, Backup não executado será exibido na coluna Status geral. Caso contrário, o status mudará para Falha no backup ou Backup bem-sucedido com base no último status do backup.

Você deve atualizar os recursos se os clusters forem renomeados fora do SnapCenter.

Adicionar recursos manualmente ao host do plug-in

A descoberta automática não é suportada no host Windows. Você deve adicionar recursos de cluster Postgresql manualmente.

Antes de começar

- Você deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts e configurar conexões do sistema de armazenamento.

Sobre esta tarefa

A descoberta automática não é suportada para as seguintes configurações:

- Layouts RDM e VMDK

Passos

1. No painel de navegação esquerdo, selecione o SnapCenter Plug-in para Postgresql na lista suspensa e clique em **Recursos**.
2. Na página Recursos, clique em **Adicionar recursos do Postgresql**.
3. Na página Fornecer detalhes do recurso, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Especifique o nome do cluster.
Nome do host	Digite o nome do host.
Tipo	Selecione o cluster.
Exemplo	Especifique o nome da instância, que é o pai do cluster.
Credenciais	Selecione as credenciais ou adicione informações para a credencial. Isto é opcional.

4. Na página Fornecer espaço de armazenamento, selecione um tipo de armazenamento e escolha um ou mais volumes, LUNs e qtrees e clique em **Salvar**.

   Opcional: Você pode clicar no * + * ícone para adicionar mais volumes, LUNs e qtrees de outros sistemas de armazenamento.

5. Opcional: Na página Configurações de Recursos, para recursos no host do Windows, insira pares de chave-valor personalizados para o plug-in PostgreSQL
6. Revise o resumo e clique em **Concluir**.

   Os clusters são exibidos junto com informações como o nome do host, grupos de recursos e políticas associados e status geral

Se você quiser fornecer aos usuários acesso aos recursos, deverá atribuir os recursos aos usuários. Isso permite que os usuários executem as ações para as quais têm permissão nos ativos atribuídos a eles.

"Adicionar um usuário ou grupo e atribuir função e ativos"

Depois que você terminar

- Depois de adicionar os clusters, você pode modificar os detalhes do cluster PostgreSQL.
- Os recursos migrados (tablespace e clusters) do SnapCenter 5.0 serão marcados como tipo de cluster PostgreSQL no SnapCenter 6.0.

- Ao modificar os recursos adicionados manualmente que são migrados do SnapCenter 5.0 ou anterior, faça o seguinte na página **Configurações de recursos** para pares de valores-chave personalizados:
  - Especifique o termo "PORT" no campo **Nome**.
  - Especifique o número da porta no campo **Valor**.

Criar políticas de backup para PostgreSQL

Antes de usar o SnapCenter para fazer backup de recursos do PostgreSQL, você deve criar uma política de backup para o recurso ou grupo de recursos que deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e mantém backups.

Antes de começar

- Você deve ter definido sua estratégia de backup.

  Para obter detalhes, consulte as informações sobre como definir uma estratégia de proteção de dados para clusters PostgreSQL.

- Você deve ter se preparado para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, configurar conexões do sistema de armazenamento e adicionar recursos.
- O administrador do SnapCenter deve ter atribuído as SVMs para os volumes de origem e destino a você se estiver replicando instantâneos para um espelho ou cofre.

  Além disso, você pode especificar configurações de replicação, script e aplicativo na política. Essas opções economizam tempo quando você deseja reutilizar a política para outro grupo de recursos.

Sobre esta tarefa

- SnapLock
  - Se a opção 'Manter as cópias de backup por um número específico de dias' for selecionada, o período de retenção do SnapLock deverá ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio de instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar à retenção de um número maior de instantâneos do que a contagem especificada na política.
  - Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Clique em **Novo**.
4. Na página Nome, insira o nome e os detalhes da política.
5. Na página Tipo de política, faça o seguinte:
   a. Selecione o tipo de armazenamento.
   b. Na seção **Configurações de backup personalizadas**, forneça quaisquer configurações de backup específicas que devem ser passadas ao plug-in no formato chave-valor.

Você pode fornecer vários valores-chave a serem passados ao plug-in.

6. Na página Backup e Replicação, execute as seguintes ações:

   a. Especifique a frequência da programação selecionando **Sob demanda**, **Por hora**, **Diariamente**, **Semanalmente** ou **Mensalmente**.

      Você pode especificar o agendamento (data de início, data de término e frequência) para a operação de backup ao criar um grupo de recursos. Isso permite que você crie grupos de recursos que compartilham a mesma política e frequência de backup, mas também permite que você atribua diferentes agendamentos de backup a cada política.

      Se você agendou para 2h00, a programação não será acionada durante o horário de verão (DST).

   a. Na seção Configurações de instantâneo, especifique as configurações de retenção para o tipo de backup e o tipo de agendamento selecionado na página **Tipo de backup**:

Se você quiser…	**Então…**
Mantenha um certo número de Snapshots	Selecione **Cópias a serem mantidas** e especifique o número de Snapshots que você deseja manter. Se o número de Snapshots exceder o número especificado, os Snapshots serão excluídos, com as cópias mais antigas sendo excluídas primeiro. Você deve definir a contagem de retenção como 2 ou mais se planeja habilitar a replicação do SnapVault . Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro Snapshot será o Snapshot de referência para o relacionamento SnapVault até que um Snapshot mais recente seja replicado para o destino. O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida como um valor maior do que o suportado pela versão do ONTAP .
Mantenha os Snapshots por um certo número de dias	Selecione **Manter cópias por** e especifique o número de dias pelos quais você deseja manter os Snapshots antes de excluí-los.

Se você quiser…	Então…
Período de bloqueio de cópia de instantâneo	Selecione **Período de bloqueio de cópia de instantâneo** e especifique dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

7. Selecione um rótulo de política.

> Você pode atribuir rótulos SnapMirror a snapshots primários para replicação remota, permitindo que os snapshots primários descarreguem a operação de replicação de snapshots do SnapCenter para sistemas secundários ONTAP . Isso pode ser feito sem habilitar a opção SnapMirror ou SnapVault na página de política.

8. Na seção Selecionar opções de replicação secundária, selecione uma ou ambas as seguintes opções de replicação secundária:

Para este campo…	Faça isso…
Atualize o SnapMirror após criar uma cópia local do Snapshot	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Se o relacionamento de proteção no ONTAP for do tipo Mirror and Vault e se você selecionar apenas esta opção, o Snapshot criado no primário não será transferido para o destino, mas será listado no destino. Se este Snapshot for selecionado no destino para executar uma operação de restauração, a seguinte mensagem de erro será exibida: O local secundário não está disponível para o backup em cofre/espelho selecionado. Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Ver "Visualize backups e clones relacionados a recursos do PostgreSQL na página Topologia" .

Para este campo…	Faça isso…
Atualize o SnapVault após criar uma cópia local do Snapshot	Selecione esta opção para executar a replicação de backup de disco para disco (backups do SnapVault). Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Quando o SnapLock é configurado somente no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página Topologia atualiza o período de bloqueio no secundário recuperado do ONTAP. Para obter mais informações sobre o SnapLock Vault, consulte Confirmar instantâneos para WORM em um destino de cofre Ver "Visualize backups e clones relacionados a recursos do PostgreSQL na página Topologia" .
Erro na contagem de novas tentativas	Insira o número máximo de tentativas de replicação que podem ser permitidas antes que a operação seja interrompida.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o armazenamento secundário para evitar atingir o limite máximo de Snapshots no armazenamento secundário.

9. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas

Um grupo de recursos é o contêiner ao qual você deve adicionar recursos que deseja fazer backup e proteger. Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente. Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que deseja executar.

Sobre esta tarefa

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Insira um nome para o grupo de recursos.  O nome do grupo de recursos não deve exceder 250 caracteres.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.
Use formato de nome personalizado para cópia de instantâneo	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do instantâneo. Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do instantâneo.

4. Na página Recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Tipo de recurso**.

   Isso ajuda a filtrar informações na tela.

5. Selecione os recursos na seção **Recursos disponíveis** e clique na seta para a direita para movê-los para a seção **Recursos selecionados**.
6. Na página Configurações do aplicativo, faça o seguinte:

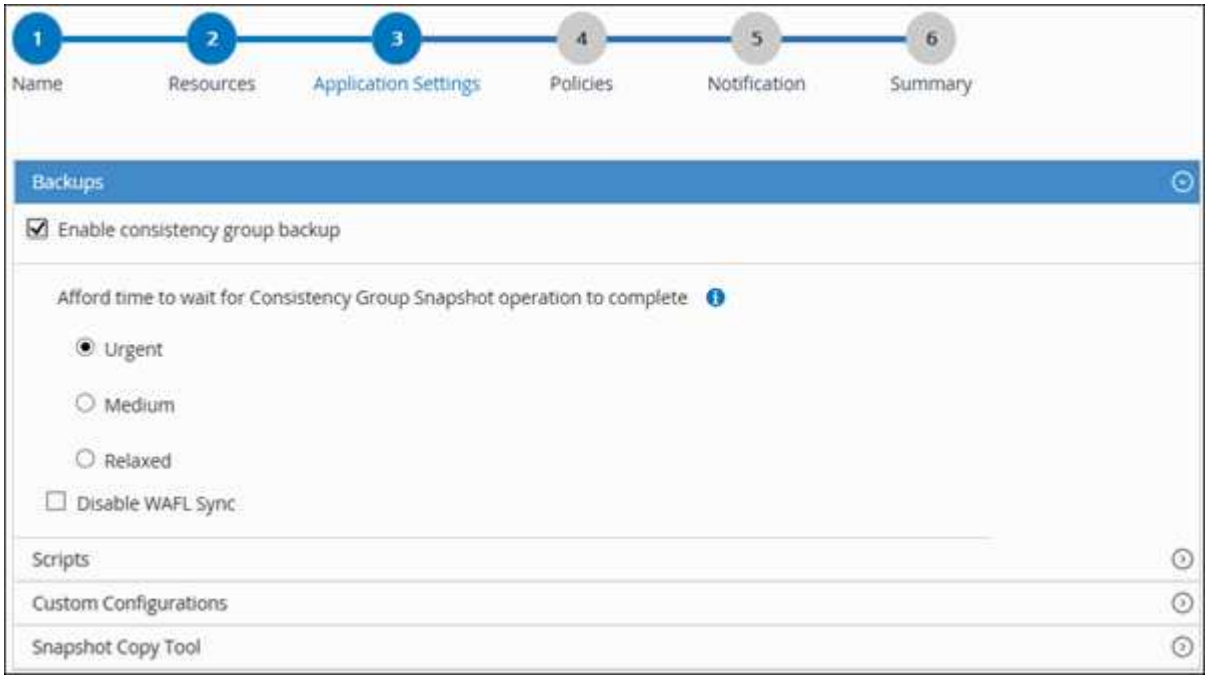
   a. Clique na seta **Backups** para definir opções adicionais de backup:

      Habilite o backup do grupo de consistência e execute as seguintes tarefas:

Para este campo…	Faça isso…
Permitir tempo para esperar a conclusão da operação de instantâneo do Consistency Group	Selecione **Urgente**, **Médio** ou **Relaxado** para especificar o tempo de espera para a conclusão da operação de instantâneo. Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.

Para este campo…	Faça isso…
Desativar sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL .

+



a. Clique na seta **Scripts** e insira os comandos pre e post para operações de inatividade, snapshot e unquiesce. Você também pode inserir os pré-comandos a serem executados antes de sair em caso de falha.

b. Clique na seta **Configurações personalizadas** e insira os pares de chave-valor personalizados necessários para todas as operações de proteção de dados que usam este recurso.

Parâmetro	Contexto	Descrição
HABILITAR_REGISTRO_DE_ARQUIVO	(S/N)	Permite que o gerenciamento de log de arquivamento exclua os logs de arquivamento.
RETENÇÃO_DE_REGISTRO_DE_ARQUIVO	número_de_dias	Especifica o número de dias que os logs de arquivamento são retidos. Esta configuração deve ser igual ou maior que NTAP_SNAPSHOT_ RETENTIONS.
DIRETÓRIO_DE_LOG_DE_ARQUIVO	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs de arquivamento.

Parâmetro	Contexto	Descrição
EXT_DE_LOG_DE_ARQUIVO	extensão_de_arquivo	Especifica o comprimento da extensão do arquivo de log de arquivamento. Por exemplo, se o log de arquivamento for log_backup_0_0_0_0.16151855 1942 9 e se o valor file_extension for 5, a extensão do log manterá 5 dígitos, que é 16151.
ARQUIVO_LOG_RECURSIVO_ SE ARQUIVO	(S/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs de arquivamento estiverem localizados em subdiretórios.

Os pares de chave-valor personalizados são suportados para sistemas de plug-in Linux do PostgreSQL e não são suportados para clusters PostgreSQL registrados como um plug-in centralizado do Windows.

c. Clique na seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar instantâneos:

Se você quiser…	Então…
SnapCenter para usar o plug-in para Windows e colocar o sistema de arquivos em um estado consistente antes de criar um snapshot. Para recursos do Linux, esta opção não é aplicável.	Selecione * SnapCenter com consistência do sistema de arquivos*.
SnapCenter para criar um instantâneo de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.
Para inserir o comando a ser executado no host para criar cópias de instantâneos.	Selecione **Outro** e insira o comando a ser executado no host para criar um instantâneo.

7. Na página Políticas, execute as seguintes etapas:

a. Selecione uma ou mais políticas na lista suspensa.

Você também pode criar uma política clicando em * + *.

As políticas são listadas na seção Configurar agendamentos para políticas selecionadas.

b. Na coluna Configurar agendamentos, clique em * + * para a política que você deseja configurar.

c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

Onde policy_name é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna **Agendamentos Aplicados**.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. O servidor SMTP deve ser configurado em **Configurações** > **Configurações globais**.

9. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e habilite proteção secundária para recursos do PostgreSQL em sistemas ASA r2

Você deve criar o grupo de recursos para adicionar os recursos que estão nos sistemas ASA r2. Você também pode provisionar a proteção secundária ao criar o grupo de recursos.

Antes de começar

- Você deve garantir que não está adicionando recursos do ONTAP 9.x e recursos do ASA r2 ao mesmo grupo de recursos.
- Você deve garantir que não tenha um banco de dados com recursos ONTAP 9.x e recursos ASA r2.

Sobre esta tarefa

- A proteção secundária estará disponível somente se o usuário conectado estiver atribuído à função que tem o recurso **SecondaryProtection** habilitado.
- Se você habilitar a proteção secundária, o grupo de recursos será colocado no modo de manutenção durante a criação dos grupos de consistência primário e secundário. Depois que os grupos de consistência primário e secundário são criados, o grupo de recursos é retirado do modo de manutenção.
- O SnapCenter não oferece suporte à proteção secundária para um recurso clone.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:
   a. Insira um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 caracteres.

   b. Insira um ou mais rótulos no campo Tag para ajudar você a pesquisar o grupo de recursos posteriormente.

Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.

c. Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

d. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

Você deve usar exatamente o mesmo destino definido no aplicativo, incluindo o prefixo, se necessário.

4. Na página Recursos, selecione o nome do host do banco de dados na lista suspensa **Host**.

Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos do ASA r2 na seção Recursos disponíveis e mova-os para a seção Recursos selecionados.
6. Na página Configurações do aplicativo, selecione a opção de backup.
7. Na página Políticas, execute as seguintes etapas:

a. Selecione uma ou mais políticas na lista suspensa.

Você também pode criar uma política clicando em + .

Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

Onde *policy_name* é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Se a proteção secundária estiver habilitada para a política selecionada, a página Proteção Secundária será exibida e você precisará executar as seguintes etapas:

a. Selecione o tipo de política de replicação.

A política de replicação síncrona não é suportada.

b. Especifique o sufixo do grupo de consistência que você deseja usar.

c. Nos menus suspensos Cluster de destino e SVM de destino, selecione o cluster emparelhado e o SVM que você deseja usar.

> O cluster e o peering de SVM não são suportados pelo SnapCenter. Você deve usar o System Manager ou as CLIs do ONTAP para executar o peering de cluster e SVM.

> Se os recursos já estiverem protegidos fora do SnapCenter, eles serão exibidos na seção Recursos Protegidos Secundários.

1. Na página Verificação, execute as seguintes etapas:

   a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para realizar a verificação no armazenamento secundário.

   b. Clique + na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política.

   c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name, execute as seguintes ações:

Se você quiser…	Faça isso…
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

   d. Selecione **Verificar no local secundário** para verificar seus backups no sistema de armazenamento secundário.

   e. Clique em **OK**.

   Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

2. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

   > Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

3. Revise o resumo e clique em **Concluir**.

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para PostgreSQL

Você deve criar uma conexão de máquina virtual de armazenamento (SVM) e uma

credencial antes de usar cmdlets do PowerShell para fazer backup, restaurar ou clonar clusters PostgreSQL.

Antes de começar

- Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.
- Você deve ter as permissões necessárias na função de administrador de infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estejam em andamento.

  As instalações do plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento porque o cache do host pode não ser atualizado e o status dos clusters pode ser exibido na GUI do SnapCenter como “Não disponível para backup” ou "`Não no armazenamento NetApp ".

- Os nomes dos sistemas de armazenamento devem ser exclusivos.

  O SnapCenter não oferece suporte a vários sistemas de armazenamento com o mesmo nome em clusters diferentes. Cada sistema de armazenamento suportado pelo SnapCenter deve ter um nome exclusivo e um endereço IP LIF de dados exclusivo.

Passos

1. Inicie uma sessão de conexão do PowerShell Core usando o cmdlet Open-SmConnection.

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

2. Crie uma nova conexão com o sistema de armazenamento usando o cmdlet Add-SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Crie uma nova credencial usando o cmdlet Add-SmCredential.

   Este exemplo mostra como criar uma nova credencial chamada FinanceAdmin com credenciais do Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Adicione o host de comunicação PostgreSQL ao SnapCenter Server.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode PostgreSQL
```

5. Instale o pacote e o plug-in SnapCenter para PostgreSQL no host.

   Para Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL
```

Para Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL -FilesystemCode scw -RunAsName FinanceAdmin
```

6. Defina o caminho para o SQLLIB.

   Para Windows, o plug-in PostgreSQL usará o caminho padrão para a pasta SQLLIB: “C:\Arquivos de Programas\IBM\SQLLIB\BIN”

   Se você quiser substituir o caminho padrão, use o seguinte comando.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
PostgreSQL -configSettings @{“PostgreSQL_SQLLIB_CMD” =
“<custom_path>\IBM\SQLLIB\BIN”}
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup do PostgreSQL

Se um recurso ainda não fizer parte de nenhum grupo de recursos, você poderá fazer backup do recurso na página Recursos.

Antes de começar

- Você deve ter criado uma política de backup.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.
- Para a operação de backup baseada em cópia de instantâneo, certifique-se de que todos os clusters de locatários sejam válidos e ativos.
- Para comandos pré e pós para operações de inatividade, instantâneo e retomada de atividade, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recurso, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Selecione * * e selecione o nome do host e o tipo de recurso para filtrar os recursos. Você pode então selecionar para fechar o painel de filtro.
3. Selecione o recurso que você deseja fazer backup.
4. Na página Recurso, selecione **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.
5. Na página Configurações do aplicativo, faça o seguinte:

   - Selecione a seta **Backups** para definir opções adicionais de backup:

     Habilite o backup do grupo de consistência, se necessário, e execute as seguintes tarefas:

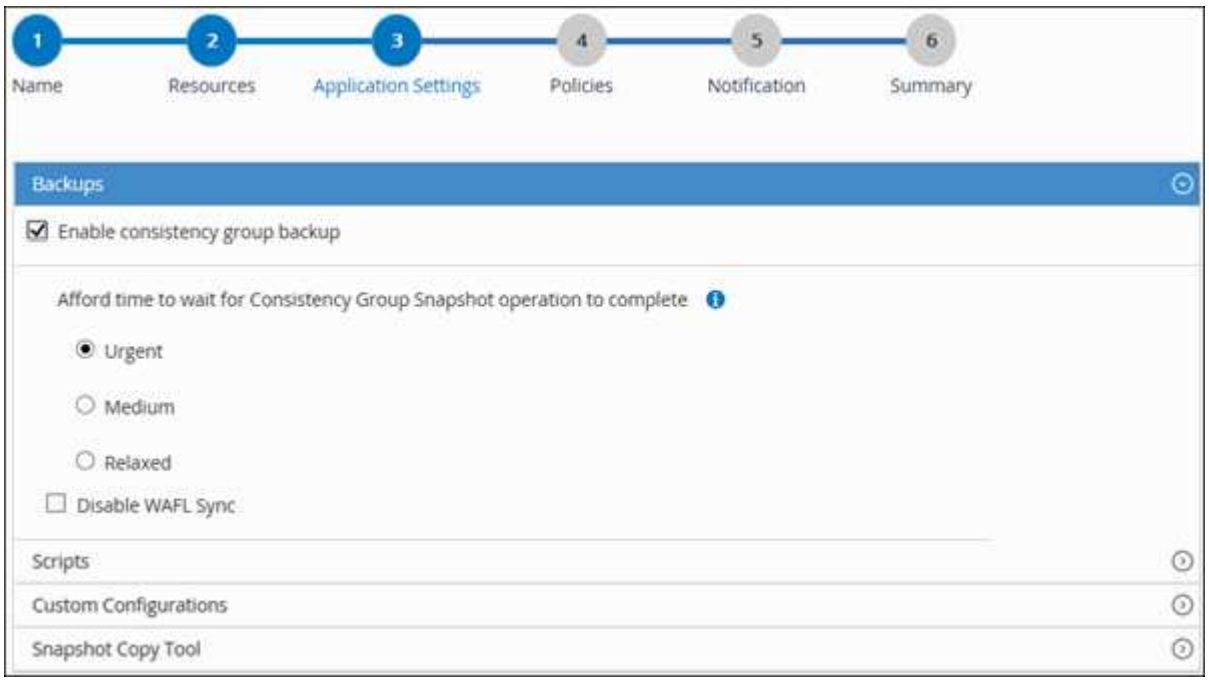
Para este campo…	Faça isso…
Permitir tempo para esperar a conclusão da operação "Consistency Group Snapshot"	Selecione **Urgente**, ou **Médio**, ou **Relaxado** para especificar o tempo de espera para a operação de Snapshot terminar. Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.
Desativar sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL .

   - Selecione a seta **Scripts** para executar comandos pré e pós para operações de inatividade, instantâneo e ativação/desativação.

     Você também pode executar pré-comandos antes de sair da operação de backup. Prescrições e pós-escritos são executados no SnapCenter Server.
   - Selecione a seta **Configurações personalizadas** e insira os pares de valores personalizados necessários para todos os trabalhos que usam este recurso.
   - Selecione a seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar Instantâneos:

Se você quiser…	Então…
SnapCenter para criar um Snapshot de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.

Se você quiser…	Então…
SnapCenter para usar o plug-in para Windows para colocar o sistema de arquivos em um estado consistente e, em seguida, criar um Snapshot	Selecione * SnapCenter com consistência do sistema de arquivos*.
Para inserir o comando para criar um Snapshot	Selecione **Outro** e insira o comando para criar um Snapshot.



6. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em * + *.

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Selecione * + * na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

   c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione **OK**.

      policy_name é o nome da política que você selecionou.

   Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

7. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. O SMTP também deve ser configurado em **Configurações** > **Configurações globais**.

8. Revise o resumo e selecione **Concluir**.

   A página de topologia de recursos é exibida.

9. Selecione **Fazer backup agora**.
10. Na página Backup, execute as seguintes etapas:
    a. Se você aplicou várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

       Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

    b. Selecione **Backup**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.
    - Nas configurações do MetroCluster , o SnapCenter pode não conseguir detectar um relacionamento de proteção após um failover.

      Para mais informações, consulte: "Não é possível detectar o relacionamento SnapMirror ou SnapVault após failover do MetroCluster"

    - Se você estiver fazendo backup de dados do aplicativo em VMDKs e o tamanho do heap Java para o SnapCenter Plug-in for VMware vSphere não for grande o suficiente, o backup poderá falhar.

      Para aumentar o tamanho do heap Java, localize o arquivo de script */opt/netapp/init_scripts/scvservice*. Nesse script, o comando *do_start method* inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: *Java -jar -Xmx8192M -Xms4096M*

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

   O prompt de nome de usuário e senha é exibido.

2. Adicione recursos manuais usando o cmdlet Add-SmResources.

   Este exemplo mostra como adicionar uma instância do PostgreSQL:

```
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. Crie uma política de backup usando o cmdlet Add-SmPolicy.
4. Proteja o recurso ou adicione um novo grupo de recursos ao SnapCenter usando o cmdlet Add-SmResourceGroup.
5. Inicie uma nova tarefa de backup usando o cmdlet New-SmBackup.

   Este exemplo mostra como fazer backup de um grupo de recursos:

   ```
   C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-
   clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
   -Policy postgresql_policy1
   ```

   Este exemplo faz backup de um recurso protegido:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
   -Policy postgresql_policy2
   ```

6. Monitore o status do trabalho (em execução, concluído ou com falha) usando o cmdlet Get-smJobSummaryReport.

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. Monitore os detalhes do trabalho de backup, como ID do backup, nome do backup para executar a operação de restauração ou clonagem usando o cmdlet Get-SmBackupReport.

```
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 :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup de grupos de recursos

Um grupo de recursos é uma coleção de recursos em um host. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos.

Antes de começar

- Você deve ter criado um grupo de recursos com uma política anexada.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.

Sobre esta tarefa

Você pode fazer backup de um grupo de recursos sob demanda na página Recursos. Se um grupo de recursos tiver uma política anexada e um agendamento configurado, os backups ocorrerão automaticamente de acordo com o agendamento.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.

   Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou selecionando e, em seguida, selecionando a tag. Você pode então selecionar para fechar o painel de filtro.

3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e selecione **Fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
   a. Se você associou várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

      Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

   b. Selecione **Backup**.
5. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Monitorar operações de backup do PostgreSQL

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Talvez você queira verificar o progresso para determinar quando ele foi concluído ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado correspondente das operações:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **Trabalhos**.
3. Na página Trabalhos, execute as seguintes etapas:

a. Clique para filtrar a lista de modo que somente as operações de backup sejam listadas.
b. Especifique as datas de início e término.
c. Na lista suspensa **Tipo**, selecione **Backup**.
d. No menu suspenso **Status**, selecione o status do backup.
e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.

4. Selecione uma tarefa de backup e clique em **Detalhes** para visualizar os detalhes da tarefa.

> Embora o status do trabalho de backup seja exibido , ao clicar em detalhes do trabalho, você poderá ver que algumas das tarefas filhas da operação de backup ainda estão em andamento ou marcadas com sinais de alerta.

5. Na página Detalhes do trabalho, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Monitore operações de proteção de dados em clusters PostgreSQL no painel Atividade

O painel Atividade exibe as cinco operações mais recentes realizadas. O painel Atividade também exibe quando a operação foi iniciada e o status da operação.

O painel Atividade exibe informações sobre operações de backup, restauração, clonagem e backup agendado.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Clique no painel Atividade para visualizar as cinco operações mais recentes.

   Quando você clica em uma das operações, os detalhes da operação são listados na página **Detalhes do trabalho**.

Cancelar operações de backup para PostgreSQL

Você pode cancelar operações de backup que estão na fila.

O que você vai precisar

- Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de backup em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** fica desabilitado para operações que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de backup enfileiradas de outros membros enquanto estiver usando essa função.

Passos

1. Execute uma das seguintes ações:

Do…	Ação
Página do monitor	a. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. b. Selecione a operação e clique em **Cancelar trabalho**.
Painel de atividades	a. Após iniciar a operação de backup, clique em * * no painel Atividade para visualizar as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

A operação é cancelada e o recurso é revertido ao estado anterior.

Visualizar backups e clones do PostgreSQL na página Topologia

Ao se preparar para fazer backup ou clonar um recurso, pode ser útil visualizar uma representação gráfica de todos os backups e clones no armazenamento primário e secundário.

Sobre esta tarefa

Você pode revisar os seguintes ícones na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no armazenamento primário ou secundário (cópias espelhadas ou cópias do Vault).

-  exibe o número de backups e clones que estão disponíveis no armazenamento primário.
-  exibe o número de backups e clones que são espelhados no armazenamento secundário usando a tecnologia SnapMirror .
-  exibe o número de backups e clones que são replicados no armazenamento secundário usando a tecnologia SnapVault .

O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou 6 backups usando uma política para manter apenas 4 backups, o número de backups exibidos será 6.

Clones de um backup de um espelho flexível em termos de versão em um volume do tipo mirror-vault são exibidos na exibição de topologia, mas a contagem de backups de espelho na exibição de topologia não inclui o backup flexível em termos de versão.

Na página Topologia, você pode ver todos os backups e clones disponíveis para o recurso ou grupo de recursos selecionado. Você pode visualizar os detalhes desses backups e clones e selecioná-los para executar operações de proteção de dados.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso na exibição de detalhes do recurso ou na exibição de detalhes do grupo de recursos.

   Se o recurso estiver protegido, a página de topologia do recurso selecionado será exibida.

4. Revise o **cartão Resumo** para ver um resumo do número de backups e clones disponíveis no armazenamento primário e secundário.

   A seção **Cartão de resumo** exibe o número total de backups baseados em cópias de instantâneo e clones.

   Clicar no botão **Atualizar** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clicar no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Uma programação semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo estiver distribuído em vários volumes, o tempo de expiração do SnapLock para o backup será o maior tempo de expiração do SnapLock definido para um Snapshot em um volume. O maior tempo de expiração do SnapLock é recuperado do ONTAP.

   Após o backup sob demanda, clicar no botão **Atualizar** atualiza os detalhes do backup ou clone.

5. Na exibição Gerenciar cópias, clique em **Backups** ou **Clones** do armazenamento primário ou secundário para ver detalhes de um backup ou clone.

   Os detalhes dos backups e clones são exibidos em formato de tabela.

6. Selecione o backup na tabela e clique nos ícones de proteção de dados para executar operações de restauração, clonagem e exclusão.

   Não é possível renomear ou excluir backups que estejam no armazenamento secundário.

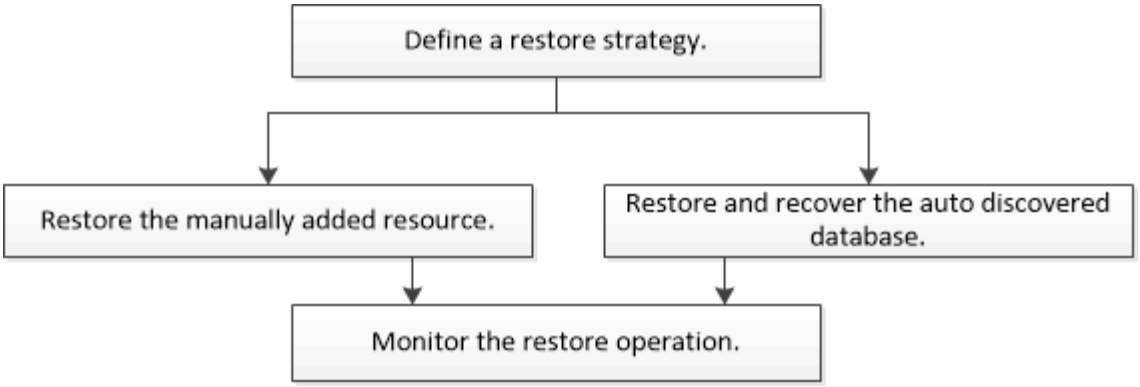
7. Se você quiser excluir um clone, selecione o clone na tabela e clique em .
8. Se você quiser dividir um clone, selecione o clone na tabela e clique em .

Restaurar PostgreSQL

Fluxo de trabalho de restauração

O fluxo de trabalho de restauração e recuperação inclui planejamento, execução de operações de restauração e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de restauração:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre os cmdlets do PowerShell.

"Guia de referência do cmdlet do software SnapCenter" .

Restaurar e recuperar um backup de recurso adicionado manualmente

Você pode usar o SnapCenter para restaurar e recuperar dados de um ou mais backups.

Antes de começar

- Você deve ter feito backup do recurso ou dos grupos de recursos.
- Você deve ter cancelado qualquer operação de backup que esteja em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos de pré-restauração, pós-restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com o tipo, host, grupos de recursos e políticas associados e status.

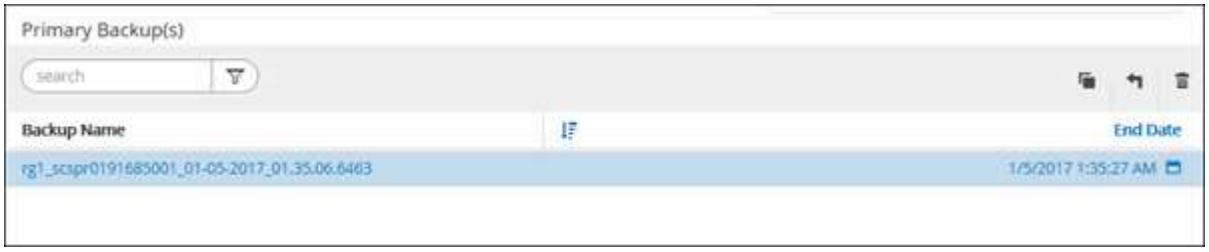
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, “Não protegido” será exibido na coluna Status geral. Isso pode significar que o recurso não está protegido ou que o backup do recurso foi feito por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e depois selecione um recurso nesse grupo.

   A página de topologia de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela Backup(s) primário(s), selecione o backup que deseja restaurar e clique em * * .



6. Na página Escopo de restauração, selecione **Recurso completo**.

   a. Se você selecionar **Recurso Completo**, todos os volumes de dados configurados do cluster PostgreSQL serão restaurados.

      Se o recurso contiver volumes ou qtrees, os Snapshots tirados após o Snapshot selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

      Você pode selecionar vários LUNs.

      Se você selecionar **Todos**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.

7. Na página Pré-operações, insira os comandos pre restore e unmount para executar antes de realizar um trabalho de restauração.

   Os comandos de desmontagem não estão disponíveis para recursos descobertos automaticamente.

8. Na página Post ops, insira os comandos mount e post restore para serem executados após realizar

um trabalho de restauração.

Os comandos de montagem não estão disponíveis para recursos descobertos automaticamente.

9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O SMTP também deve ser configurado na página **Configurações** > **Configurações globais**.

10. Revise o resumo e clique em **Concluir**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
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
```

   Este exemplo exibe informações detalhadas sobre o backup de 29 de janeiro de 2015 a 3 de fevereiro de 2015:

```
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. Restaure os dados do backup usando o cmdlet Restore-SmBackup.

```
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          :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Restaurar e recuperar um backup de cluster descoberto automaticamente

Você pode usar o SnapCenter para restaurar e recuperar dados de um ou mais backups.

Antes de começar

- Você deve ter feito backup do recurso ou dos grupos de recursos.
- Você deve ter cancelado qualquer operação de backup que esteja em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos de pré-restauração, pós-restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-*

in Creator\etc\allowed_commands.config

- Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Cópias de backup baseadas em arquivo não podem ser restauradas do SnapCenter.
- Para recursos descobertos automaticamente, a restauração é suportada com SFSR.
- A recuperação automática não é suportada.
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com o tipo, host, grupos de recursos e políticas associados e status.

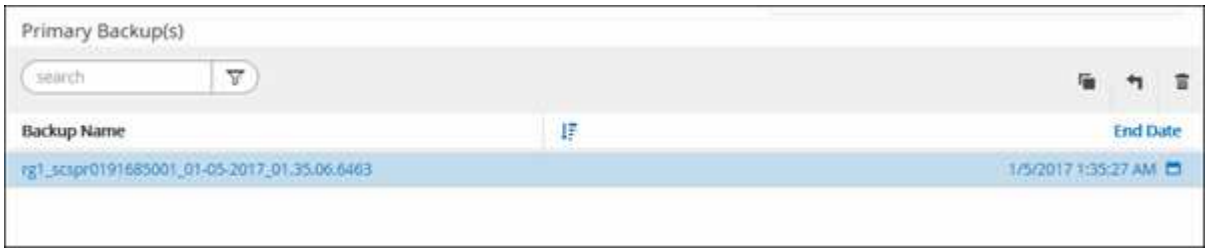
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, “Não protegido” será exibido na coluna Status geral. Isso pode significar que o recurso não está protegido ou que o backup do recurso foi feito por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e depois selecione um recurso nesse grupo.

   A página de topologia de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela Backup(s) primário(s), selecione o backup que deseja restaurar e clique em * * .



6. Na página Escopo de restauração, selecione **Recurso completo** para restaurar os volumes de dados configurados do cluster PostgreSQL.
7. Na página Escopo de recuperação, selecione uma das seguintes opções:

Se você…	Faça isso…

Quer recuperar o mais próximo possível do tempo atual	Selecione **Recuperar para o estado mais recente**. Para recursos de contêiner único, especifique um ou mais locais de backup de log e catálogo.
Deseja recuperar até o ponto especificado no tempo	Selecione **Recuperar para um ponto no tempo**. a. Insira a data e a hora. Insira a data e a hora. Por exemplo, o host PostgreSQL Linux está localizado em Sunnyvale, CA, e o usuário em Raleigh, NC, está recuperando os logs no SnapCenter. Se o usuário quiser executar uma recuperação para 5h da manhã em Sunnyvale, CA, o usuário deverá definir o fuso horário do navegador para o fuso horário do host Linux PostgreSQL, que é GMT-07:00 e especificar a data e a hora como 5h da manhã.
Não quero recuperar	Selecione **Sem recuperação**.

Não é possível recuperar recursos do PostgreSQL adicionados manualmente.

O plug-in SnapCenter para PostgreSQL cria um backup_label e um tablespace_map na pasta */<OS_temp_folder>/postgresql_sc_recovery*<Restore_JobId>/_ para ajudar na recuperação manual.

1. Na página Pré-operações, insira os comandos pre restore e unmount para executar antes de realizar um trabalho de restauração.

   Os comandos de desmontagem não estão disponíveis para recursos descobertos automaticamente.

2. Na página Post ops, insira os comandos mount e post restore para serem executados após realizar um trabalho de restauração.

   Os comandos de montagem não estão disponíveis para recursos descobertos automaticamente.

3. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O SMTP também deve ser configurado na página **Configurações** > **Configurações globais**.

4. Revise o resumo e clique em **Concluir**.
5. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Restaurar recursos usando cmdlets do PowerShell

Restaurar um backup de recursos inclui iniciar uma sessão de conexão com o SnapCenter Server, listar os backups e recuperar informações de backup, além de

restaurar um backup.

Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
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
```

   Este exemplo exibe informações detalhadas sobre o backup de 29 de janeiro de 2015 a 3 de fevereiro de 2015:

```
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. Restaure os dados do backup usando o cmdlet Restore-SmBackup.

```
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           :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitorar operações de restauração do PostgreSQL

Você pode monitorar o progresso de diferentes operações de restauração do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa tomar.

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento

- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de restauração sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Restaurar**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Aplicar** para visualizar as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Clonar backups de recursos do PostgreSQL

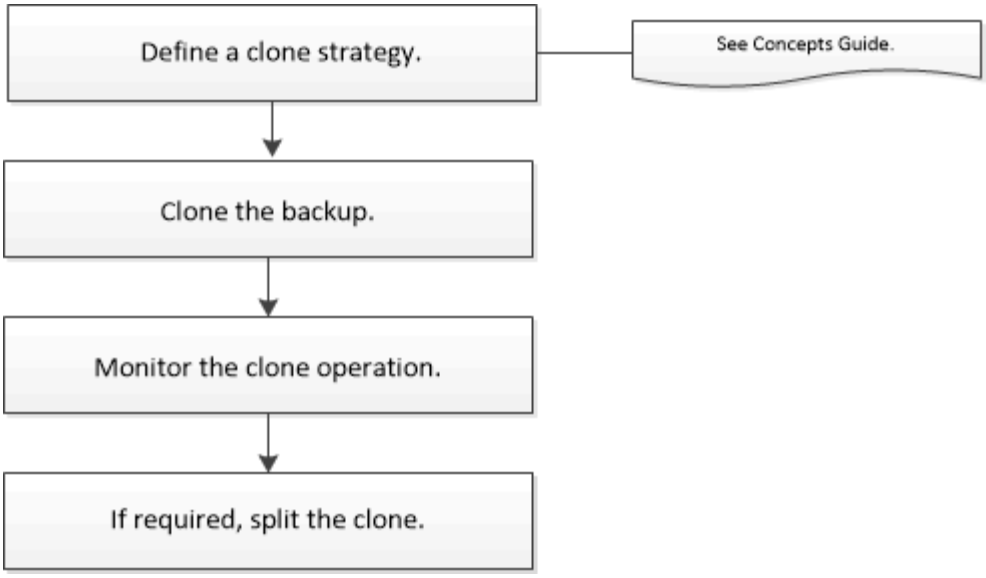
Fluxo de trabalho de clonagem

O fluxo de trabalho de clonagem inclui executar a operação de clonagem e monitorar a operação.

Sobre esta tarefa

- Você pode clonar no servidor PostgreSQL de origem.
- Você pode clonar backups de recursos pelos seguintes motivos:
  - Para testar a funcionalidade que deve ser implementada usando a estrutura e o conteúdo atuais dos recursos durante os ciclos de desenvolvimento do aplicativo
  - Para ferramentas de extração e manipulação de dados ao preencher data warehouses
  - Para recuperar dados que foram excluídos ou alterados por engano

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de clonagem:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre os cmdlets do PowerShell.

Clonar um backup do PostgreSQL

Você pode usar o SnapCenter para clonar um backup. Você pode clonar a partir do backup primário ou secundário.

Antes de começar

- Você deve ter feito backup dos recursos ou do grupo de recursos.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de armazenamento (SVM).
- Para comandos de pré-clonagem ou pós-clonagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Para obter informações sobre as operações de divisão de volume do FlexClone , consultehttps://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html["Dividir um volume FlexClone de seu volume pai"] .
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com informações como tipo, host, grupos de recursos e políticas associados e status.

3. Selecione o recurso ou grupo de recursos.

   Você deve selecionar um recurso se selecionar um grupo de recursos.

   A página de topologia de recurso ou grupo de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Selecione o backup de dados da tabela e clique em  .
6. Na página Localização, execute as seguintes ações:

Para este campo…	Faça isso…
Servidor clone	Escolha um host no qual o clone deve ser criado.
Porto de destino	Insira a porta de destino do PostgreSQL a ser clonada a partir dos backups existentes.
Endereço IP de exportação NFS	Insira os endereços IP ou os nomes de host nos quais os volumes clonados serão exportados. Isso é aplicável somente ao recurso do tipo de armazenamento NFS.
Pool de Capacidade Máxima Taxa de Transferência (MiB/s)	Insira a taxa de transferência máxima de um pool de capacidade. Isso é aplicável somente ao recurso do tipo de armazenamento ANF.

7. Na página Scripts, execute as seguintes etapas:

   Os scripts são executados no host do plug-in.

   a. Insira os comandos para pré-clonagem ou pós-clonagem que devem ser executados antes ou depois da operação de clonagem, respectivamente.
      - Comando pré-clone: exclui clusters existentes com o mesmo nome
      - Comando pós-clone: verificar um cluster ou iniciar um cluster.
   b. Digite o comando mount para montar um sistema de arquivos em um host.

Comando de montagem para um volume ou qtree em uma máquina Linux:

Exemplo para NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail.

9. Revise o resumo e clique em **Concluir**.
10. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

2. Recupere os backups para executar a operação de clonagem usando o cmdlet Get-SmBackup.

   Este exemplo mostra que dois backups estão disponíveis para clonagem:

```
 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. Inicie uma operação de clonagem a partir de um backup existente e especifique os endereços IP de exportação do NFS nos quais os volumes clonados serão exportados.

   Este exemplo mostra que o backup a ser clonado tem um endereço NFSExportIPs de 10.32.212.14:

   Para cluster PostgreSQL:

```
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
```

Se NFSExportIPs não for especificado, o padrão será exportado para o host de destino do clone.

4. Verifique se os backups foram clonados com sucesso usando o cmdlet Get-SmCloneReport para visualizar os detalhes do trabalho de clonagem.

   Você pode visualizar detalhes como ID do clone, data e hora de início, data e hora de término.

```
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          :
```

Monitorar operações de clonagem do PostgreSQL

Você pode monitorar o progresso das operações de clonagem do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente operações de clonagem sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione o trabalho de clonagem e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página Detalhes do trabalho, clique em **Exibir registros**.

Dividir um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido se torna independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clone em um clone intermediário.

  Por exemplo, depois de criar o clone1 a partir de um backup de banco de dados, você pode criar um backup do clone1 e então clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e você não pode executar a operação de divisão de clone no clone1. No entanto, você pode executar a operação de divisão de clone no clone2.

  Após dividir o clone2, você pode executar a operação de divisão do clone no clone1 porque o clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e os trabalhos de clonagem do clone são excluídos.
- Para obter informações sobre as operações de divisão de volume do FlexClone , consulte "Dividir um volume FlexClone de seu volume pai" .
- Certifique-se de que o volume ou agregado no sistema de armazenamento esteja online.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.

2. Na página **Recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicações de banco de dados	Selecione **Banco de dados** na lista Exibir.
Para sistemas de arquivos	Selecione **Caminho** na lista Exibir.

3. Selecione o recurso apropriado na lista.

   A página de topologia de recursos é exibida.

4. Na exibição **Gerenciar cópias**, selecione o recurso clonado (por exemplo, o banco de dados ou LUN) e clique em *  *.
5. Revise o tamanho estimado do clone que será dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

   A operação de divisão do clone para de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clone e, em seguida, tentar novamente a operação de divisão de clone.

   Se você quiser um tempo de pesquisa maior ou menor para verificar se o clone está dividido ou não, você pode alterar o valor do parâmetro *CloneSplitStatusCheckPollTime* no arquivo *SMCoreServiceHost.exe.config* para definir o intervalo de tempo para o SMCore pesquisar o status da operação de divisão do clone. O valor está em milissegundos e o valor padrão é 5 minutos.

   Por exemplo:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   A operação de início da divisão do clone falha se um backup, uma restauração ou outra divisão do clone estiver em andamento. Você deve reiniciar a operação de divisão do clone somente após a conclusão das operações em execução.

Informações relacionadas

"O clone ou a verificação do SnapCenter falham com o agregado inexistente"

Excluir ou dividir clones de cluster do PostgreSQL após atualizar o SnapCenter

Após atualizar para o SnapCenter 4.3, você não verá mais os clones. Você pode excluir o clone ou dividir os clones na página Topologia do recurso a partir do qual os clones foram criados.

Sobre esta tarefa

Se você quiser localizar a pegada de armazenamento dos clones ocultos, execute o seguinte comando: `Get-SmClone -ListStorageFootprint`

Passos

1. Exclua os backups dos recursos clonados usando o cmdlet remove-smbackup.
2. Exclua o grupo de recursos dos recursos clonados usando o cmdlet remove-smresourcegroup.
3. Remova a proteção do recurso clonado usando o cmdlet remove-smprotectresource.
4. Selecione o recurso pai na página Recursos.

   A página de topologia de recursos é exibida.

5. Na exibição Gerenciar cópias, selecione os clones dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
6. Selecione os clones e clique em  para excluir clones ou clicar  para dividir os clones.
7. Clique em **OK**.

Proteger MySQL

Plug-in SnapCenter para MySQL

Visão geral do plug-in SnapCenter para MySQL

O plug-in SnapCenter para banco de dados MySQL é um componente do lado do host do SnapCenter software NetApp SnapCenter que permite o gerenciamento de proteção de dados com reconhecimento de aplicativo de bancos de dados MySQL. O plug-in para banco de dados MySQL automatiza o backup, a restauração e a clonagem de bancos de dados MySQL no seu ambiente SnapCenter .

O SnapCenter oferece suporte a configurações de instância única do MySQL. Você pode usar o Plug-in para Banco de Dados MySQL em ambientes Linux e Windows. Em ambientes Windows, o MySQL será suportado como recurso manual.

Quando o Plug-in para Banco de Dados MySQL estiver instalado, você poderá usar o SnapCenter com a tecnologia NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume. Você também pode usar o plug-in com a tecnologia NetApp SnapVault para executar a replicação de backup de disco para disco para conformidade com os padrões.

O plug-in SnapCenter para MySQL oferece suporte a NFS e SAN em layouts de armazenamento de arquivos ONTAP e Azure NetApp .

O layout de armazenamento virtual VMDK, vVol e RDM é suportado.

Links simbólicos não são suportados.

O que você pode fazer usando o plug-in SnapCenter para MySQL

Ao instalar o Plug-in para Banco de Dados MySQL em seu ambiente, você pode usar o SnapCenter para fazer backup, restaurar e clonar instâncias do MySQL. Você também pode executar tarefas de suporte a essas operações.

- Adicionar instâncias.
- Crie backups.
- Restaurar a partir de backups.
- Clonar backups.
- Agende operações de backup.
- Monitore operações de backup, restauração e clonagem.
- Visualize relatórios de operações de backup, restauração e clonagem.

Recursos do plug-in SnapCenter para MySQL

O SnapCenter integra-se ao aplicativo plug-in e às tecnologias NetApp no sistema de armazenamento. Para trabalhar com o Plug-in para Banco de Dados MySQL, use a interface gráfica do usuário do SnapCenter .

- **Interface gráfica de usuário unificada**

  A interface do SnapCenter fornece padronização e consistência entre plug-ins e ambientes. A interface do SnapCenter permite que você conclua operações consistentes de backup, restauração e clonagem em plug-ins, use relatórios centralizados, use visualizações de painel rápidas, configure o controle de acesso baseado em função (RBAC) e monitore trabalhos em todos os plug-ins.

- **Administração central automatizada**

  Você pode agendar operações de backup, configurar retenção de backup baseada em políticas e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- *Tecnologia de cópia instantânea não disruptiva da NetApp *

  O SnapCenter usa a tecnologia de snapshot da NetApp com o Plug-in para Banco de Dados MySQL para fazer backup de recursos.

Usar o Plug-in para MySQL também oferece os seguintes benefícios:

- Suporte para fluxos de trabalho de backup, restauração e clonagem
- Segurança com suporte RBAC e delegação centralizada de funções

  Você também pode definir as credenciais para que os usuários autorizados do SnapCenter tenham permissões no nível do aplicativo.

- Criação de cópias de recursos com eficiência de espaço e em um determinado momento para testes ou extração de dados usando a tecnologia NetApp FlexClone

  Uma licença FlexClone é necessária no sistema de armazenamento onde você deseja criar o clone.

- Suporte para o recurso de instantâneo do grupo de consistência (CG) do ONTAP como parte da criação de backups.
- Capacidade de executar vários backups simultaneamente em vários hosts de recursos

  Em uma única operação, os snapshots são consolidados quando recursos em um único host compartilham o mesmo volume.

- Capacidade de criar snapshots usando comandos externos.
- Suporte para Linux LVM no sistema de arquivos XFS.

Tipos de armazenamento suportados pelo SnapCenter Plug-in para MySQL

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e virtuais (VMs). Você deve verificar o suporte para seu tipo de armazenamento antes de instalar o SnapCenter Plug-in para MySQL.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados por FC • LUNs conectados por iSCSI • Volumes conectados ao NFS
VMware ESXi	• LUNs RDM conectados por um FC ou iSCSI ESXi HBAA varredura de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluída porque o SnapCenter verifica todos os adaptadores de barramento de host presentes no host. Você pode editar o arquivo **LinuxConfig.pm** localizado em */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* para definir o valor do parâmetro **SCSI_HOSTS_OPTIMIZED_RESCAN** como 1 para verificar novamente apenas os HBAs listados em HBA_DRIVER_NAMES. • LUNs iSCSI conectados diretamente ao sistema convidado pelo iniciador iSCSI • VMDKs em armazenamentos de dados NFS • VMDKs em VMFS criados • Volumes NFS conectados diretamente ao sistema convidado • Armazenamentos de dados vVol em NFS e SAN O armazenamento de dados vVol só pode ser provisionado com o ONTAP Tools para VMware vSphere.

Privilégios ONTAP mínimos necessários para o plug-in MySQL

Os privilégios mínimos do ONTAP necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos de acesso total: privilégios mínimos necessários para ONTAP 9.12.1 e posterior
  - evento generate-autosupport-log
  - histórico de trabalho mostrar
  - parada de trabalho
  - lua
  - lun criar
  - lun criar
  - lun criar

- lun delete
- lun igroup adicionar
- lun igroup criar
- lun igroup excluir
- renomear lun igroup
- renomear lun igroup
- show do lun igroup
- mapeamento lun add-reporting-nodes
- criação de mapeamento lun
- exclusão de mapeamento lun
- mapeamento lun remove-reporting-nodes
- show de mapeamento lunar
- lun modificar
- volume de entrada lun
- lua offline
- lua online
- lun persistente-reserva clara
- redimensionamento de lun
- série lun
- show de lua
- política de adição de regra do snapmirror
- regra de modificação de política do snapmirror
- política de remoção do snapmirror
- política do snapmirror mostrar
- restauração do snapmirror
- show de espelhos instantâneos
- histórico de exibição do snapmirror
- atualização do snapmirror
- atualização do snapmirror-ls-set
- lista-destinos do snapmirror
- versão
- criação de clone de volume
- show de clones de volume
- volume clone split start
- volume clone divisão parada
- volume criar
- destruição de volume

    - clone de arquivo de volume criar
    - arquivo de volume mostrar-uso-do-disco
    - volume offline
    - volume on-line
    - modificação de volume
    - volume qtree criar
    - volume qtree delete
    - volume qtree modificar
    - volume qtree mostrar
    - restrição de volume
    - show de volume
    - criação de instantâneo de volume
    - exclusão de instantâneo de volume
    - modificação de instantâneo de volume
    - instantâneo de volume modificar-tempo-de-expiração-do-snaplock
    - renomeação de instantâneo de volume
    - restauração de instantâneo de volume
    - arquivo de restauração de instantâneo de volume
    - exibição de instantâneo de volume
    - desmontagem de volume
    - cifs do vserver
    - vserver cifs compartilhar criar
    - vserver cifs compartilhar excluir
    - vserver cifs shadowcopy mostrar
    - vserver cifs compartilhar mostrar
    - vserver cifs mostrar
    - política de exportação do vserver
    - criação de política de exportação do vserver
    - exclusão da política de exportação do vserver
    - criação de regra de política de exportação do vserver
    - mostrar regra de política de exportação do vserver
    - mostrar política de exportação do vserver
    - vserver iscsi
    - mostrar conexão iscsi do vserver
    - vserver mostrar
- Comandos somente leitura: privilégios mínimos necessários para ONTAP 8.3.0 e posterior
    - interface de rede

- exibição de interface de rede
- vserver

Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para MySQL

Você pode usar um plug-in SnapCenter com a tecnologia ONTAP SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia ONTAP SnapVault para executar replicação de backup de disco para disco para conformidade com padrões e outros propósitos relacionados à governança. Antes de executar essas tarefas, você deve configurar um relacionamento de proteção de dados entre os volumes de origem e destino e inicializar o relacionamento.

O SnapCenter executa as atualizações no SnapMirror e no SnapVault após concluir a operação Snapshot. As atualizações do SnapMirror e do SnapVault são executadas como parte do trabalho do SnapCenter ; não crie uma programação ONTAP separada.

Se você estiver acessando o SnapCenter a partir de um produto NetApp SnapManager e estiver satisfeito com os relacionamentos de proteção de dados configurados, pode pular esta seção.

Um relacionamento de proteção de dados replica dados do armazenamento primário (o volume de origem) para o armazenamento secundário (o volume de destino). Quando você inicializa o relacionamento, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não oferece suporte a relacionamentos em cascata entre volumes SnapMirror e SnapVault (**Primário** > **Espelho** > **Cofre**). Você deve usar relacionamentos fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis em termos de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis em termos de versão e como configurá-los, consulte "Documentação do ONTAP" .

Estratégia de backup para MySQL

Definir uma estratégia de backup para MySQL

Definir uma estratégia de backup antes de criar suas tarefas de backup ajuda você a ter os backups necessários para restaurar ou clonar seus recursos com sucesso. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (RTO) e objetivo de ponto de recuperação (RPO) determinam em grande parte sua estratégia de backup.

Sobre esta tarefa

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. RTO é o tempo em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. SLA, RTO e RPO contribuem para a estratégia de proteção de dados.

Passos

1. Determine quando você deve fazer backup dos seus recursos.
2. Decida quantos trabalhos de backup você precisa.
3. Decida como nomear seus backups.
4. Decida se você deseja criar uma política baseada em cópia de instantâneo para fazer backup de instantâneos consistentes com o aplicativo do banco de dados.
5. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção de longo prazo.
6. Determine o período de retenção dos snapshots no sistema de armazenamento de origem e no destino do SnapMirror .
7. Determine se você deseja executar algum comando antes ou depois da operação de backup e forneça uma prescrição ou pós-escrito.

Descoberta automática de recursos no host Linux

Os recursos são instâncias do MySQL no host Linux que são gerenciadas pelo SnapCenter. Após instalar o plug-in SnapCenter Plug-in para MySQL, as instâncias do MySQL naquele host Linux são descobertas automaticamente e exibidas na página Recursos.

Tipo de backups suportados

O tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter oferece suporte ao tipo de backup baseado em cópia de snapshot para bancos de dados MySQL.

Backup baseado em cópia instantânea

Os backups baseados em cópias de instantâneo aproveitam a tecnologia de instantâneo da NetApp para criar cópias on-line somente leitura dos volumes nos quais os bancos de dados MySQL residem.

Como o plug-in SnapCenter para MySQL usa instantâneos de grupo de consistência

Você pode usar o plug-in para criar instantâneos de grupos de consistência para grupos de recursos. Um grupo de consistência é um contêiner que pode abrigar vários volumes para que você possa gerenciá-los como uma única entidade. Um grupo de consistência é composto por instantâneos simultâneos de vários volumes, fornecendo cópias consistentes de um grupo de volumes.

Você também pode especificar o tempo de espera para que o controlador de armazenamento agrupe snapshots de forma consistente. As opções de tempo de espera disponíveis são **Urgente**, **Médio** e **Relaxado**. Você também pode habilitar ou desabilitar a sincronização do Write Anywhere File Layout (WAFL) durante a operação consistente de snapshot de grupo. A sincronização do WAFL melhora o desempenho de um instantâneo de grupo de consistência.

Como o SnapCenter gerencia a manutenção de backups de log

O SnapCenter gerencia a manutenção de backups de dados nos níveis do sistema de armazenamento e do sistema de arquivos.

Considerações para determinar agendamentos de backup para MySQL

O fator mais crítico na determinação de um cronograma de backup é a taxa de alteração do recurso. Você pode fazer backup de um recurso muito utilizado a cada hora, enquanto pode fazer backup de um recurso raramente utilizado uma vez por dia. Outros fatores incluem a importância do recurso para sua organização, seu acordo de nível de serviço (SLA) e seu objetivo de ponto de recuperação (RPO).

Os agendamentos de backup têm duas partes, conforme a seguir:

- Frequência de backup (com que frequência os backups devem ser realizados)

  A frequência de backup, também chamada de tipo de agendamento para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como horária, diária, semanal ou mensal.

- Agendamentos de backup (exatamente quando os backups devem ser executados)

  Os agendamentos de backup fazem parte de uma configuração de recurso ou grupo de recursos. Por exemplo, se você tiver um grupo de recursos com uma política configurada para backups semanais, poderá configurar o agendamento para fazer backup todas as quintas-feiras às 22h.

Número de trabalhos de backup necessários para o MySQL

Os fatores que determinam o número de tarefas de backup necessárias incluem o tamanho do recurso, o número de volumes usados, a taxa de alteração do recurso e seu Contrato de Nível de Serviço (SLA).

Convenções de nomenclatura de backup para plug-ins de bancos de dados MySQL

Você pode usar a convenção de nomenclatura padrão do Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um registro de data e hora aos nomes de instantâneos que ajuda a identificar quando as cópias foram criadas.

O Snapshot usa a seguinte convenção de nomenclatura padrão:

```
resourcegroupname_hostname_timestamp
```

Você deve nomear seus grupos de recursos de backup logicamente, como no exemplo a seguir:

```
dts1_mach1x88_03-12-2015_23.17.26
```

Neste exemplo, os elementos de sintaxe têm os seguintes significados:

- *dts1* é o nome do grupo de recursos.
- *mach1x88* é o nome do host.
- *03-12-2015_23.17.26* é a data e o registro de data e hora.

Como alternativa, você pode especificar o formato do nome do Snapshot ao proteger recursos ou grupos de recursos selecionando **Usar formato de nome personalizado para cópia do Snapshot**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do registro de data e hora é adicionado ao nome do Snapshot.

Estratégia de restauração e recuperação para MySQL

Definir uma estratégia de restauração e recuperação para recursos MySQL

Você deve definir uma estratégia antes de restaurar e recuperar seu banco de dados para que possa executar operações de restauração e recuperação com sucesso.

Somente a recuperação manual do banco de dados é suportada.

Passos

1. Determinar as estratégias de restauração suportadas para recursos MySQL adicionados manualmente
2. Determinar as estratégias de restauração suportadas para bancos de dados MySQL descobertos automaticamente
3. Decida o tipo de operações de recuperação que você deseja executar.

Tipos de estratégias de restauração suportadas para recursos MySQL adicionados manualmente

Você deve definir uma estratégia antes de poder executar com sucesso operações de restauração usando o SnapCenter. Existem dois tipos de estratégias de restauração para recursos MySQL adicionados manualmente.

Não é possível recuperar recursos MySQL adicionados manualmente.

Restauração completa de recursos

- Restaura todos os volumes, qtrees e LUNs de um recurso

Se o recurso contiver volumes ou qtrees, os instantâneos tirados após o instantâneo selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

Tipo de estratégia de restauração suportada para MySQL descoberto automaticamente

Você deve definir uma estratégia antes de poder executar com sucesso operações de restauração usando o SnapCenter.

A restauração completa de recursos é a estratégia de restauração suportada por bancos de dados MySQL descobertos automaticamente. Isso restaura todos os volumes, qtrees e LUNs de um recurso.

Tipos de operações de restauração para MySQL descoberto automaticamente

O plug-in SnapCenter para MySQL oferece suporte a Single File SnapRestore e tipos de restauração de conexão e cópia para bancos de dados MySQL descobertos

automaticamente.

O Single File SnapRestore é executado em ambientes NFS para os seguintes cenários:

- Se apenas a opção **Recurso Completo** for selecionada
- Quando o backup selecionado for de um local secundário do SnapMirror ou SnapVault e a opção **Recurso Completo** for selecionada

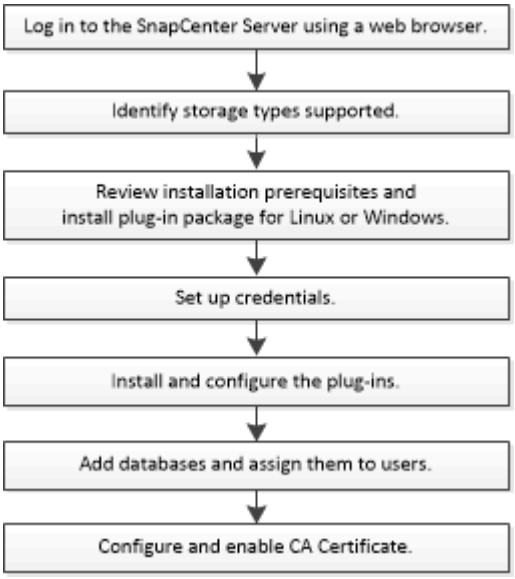
O Single File SnapRestore é executado em ambientes SAN para os seguintes cenários:

- Se apenas a opção **Recurso Completo** for selecionada
- Quando o backup é selecionado de um local secundário do SnapMirror ou SnapVault e a opção **Recurso Completo** é selecionada

Prepare-se para instalar o plug-in SnapCenter para MySQL

Fluxo de trabalho de instalação do plug-in SnapCenter para MySQL

Você deve instalar e configurar o SnapCenter Plug-in para MySQL se quiser proteger bancos de dados MySQL.



Pré-requisitos para adicionar hosts e instalar o SnapCenter Plug-in para MySQL

Antes de adicionar um host e instalar os pacotes de plug-in, você deve concluir todos os requisitos. O plug-in SnapCenter para MySQL está disponível em ambientes Windows e Linux.

- Você deve ter instalado o Java 11 no seu host.

  O IBM Java não é suportado em hosts Windows e Linux.

- No Windows, o Plug-in Creator Service deve ser executado usando o usuário do Windows “LocalSystem”, que é o comportamento padrão quando o Plug-in para MySQL é instalado como administrador de domínio.

- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host. O plug-in SnapCenter para Microsoft Windows será implantado por padrão com o plug-in MySQL em hosts Windows.
- O SnapCenter Server deve ter acesso à porta 8145 ou personalizada do host do Plug-in para MySQL.
- Para o MySQL 5.7, o binlog deve ser especificado no arquivo de configuração do mysql (my.cnf ou mysql-server.cnf).

Hosts do Windows

- Você deve ter um usuário de domínio com privilégios de administrador local e permissões de login local no host remoto.
- Ao instalar o Plug-in para MySQL em um host Windows, o SnapCenter Plug-in para Microsoft Windows é instalado automaticamente.
- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 no seu host Windows.

  "Baixe JAVA para todos os sistemas operacionais"

  "Ferramenta de Matriz de Interoperabilidade da NetApp"

Hosts Linux

- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 no seu host Linux.

  "Baixe JAVA para todos os sistemas operacionais"

  "Ferramenta de Matriz de Interoperabilidade da NetApp"

- Para bancos de dados MySQL em execução em um host Linux, ao instalar o Plug-in para MySQL, o SnapCenter Plug-in para UNIX é instalado automaticamente.
- Você deve ter **bash** como o shell padrão para instalação de plug-ins.

Comandos suplementares

Para executar um comando suplementar no SnapCenter Plug-in para MySQL, você deve incluí-lo no arquivo *allowed_commands.config*.

- Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Para permitir comandos suplementares no host do plug-in, abra o arquivo *allowed_commands.config* em um editor. Digite cada comando em uma linha separada e os comandos não diferenciam maiúsculas de minúsculas. Certifique-se de especificar o caminho totalmente qualificado e coloque-o entre aspas (") se ele contiver espaços.

Por exemplo:

comando: mount comando: umount comando: "C:\Arquivos de Programas\ NetApp\SnapCreator

commands\sdcli.exe" comando: myscript.bat

Se o arquivo *allowed_commands.config* não estiver presente, os comandos ou a execução do script serão bloqueados e o fluxo de trabalho falhará com o seguinte erro:

"[/mnt/mount -a] execução não permitida. Autorize adicionando o comando no arquivo %s no host do plugin."

Se o comando ou script não estiver presente no *allowed_commands.config*, a execução do comando ou script será bloqueada e o fluxo de trabalho falhará com o seguinte erro:

"[/mnt/mount -a] execução não permitida. Autorize adicionando o comando no arquivo %s no host do plugin."

Você não deve usar uma entrada curinga (*) para permitir todos os comandos.

Configurar privilégios sudo para usuários não root para host Linux

O SnapCenter permite que um usuário não root instale o pacote de plug-ins do SnapCenter para Linux e inicie o processo de plug-in. Os processos do plug-in serão executados como um usuário não root efetivo. Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se a umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro dela tenham permissão de 555. Caso contrário, a instalação do plug-in poderá falhar.
- Para o usuário não root, certifique-se de que o nome do usuário não root e o nome do grupo do usuário sejam os mesmos.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos do código de autenticação de mensagens: MACs hmac-sha2-256 e MACs hmac-sha2-512.

  Reinicie o serviço sshd após atualizar o arquivo de configuração.

  Exemplo:

```
#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
```

Sobre esta tarefa

Você deve configurar privilégios sudo para que o usuário não root forneça acesso aos seguintes caminhos:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /localização_personalizada/ NetApp/snapcenter/spl/instalação/plugins/desinstalação
- /localização_personalizada/ NetApp/snapcenter/spl/bin/spl

Passos

1. Efetue login no host Linux no qual você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
2. Adicione as seguintes linhas ao arquivo /etc/sudoers usando o utilitário visudo Linux.

```
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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Se você tiver uma configuração RAC, junto com os outros comandos permitidos, você deve adicionar o seguinte ao arquivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Você pode obter o valor de *crs_home* do arquivo */etc/oracle/olr.loc*.

LINUX_USER é o nome do usuário não root que você criou.

Você pode obter o *checksum_value* do arquivo **sc_unix_plugins_checksum.txt**, localizado em:

- _C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _ se o SnapCenter Server estiver instalado no host Windows.
- _/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ se o SnapCenter Server estiver instalado no host Linux.

O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows

Antes de instalar o pacote de plug-ins do SnapCenter para Windows, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas Operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	5 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell Core 7.4.2 Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux

Antes de instalar o pacote de plug-ins SnapCenter para Linux, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas operacionais	• Red Hat Enterprise Linux • Servidor SUSE Linux Enterprise (SLES) Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	2 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	Java 11 Oracle Java e OpenJDK Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em /var/opt/snapcenter/spl/etc/spl.properties esteja definida para a versão correta do JAVA e o caminho correto. Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Configurar credenciais para o plug-in SnapCenter para MySQL

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter . Você deve criar credenciais para instalar plug-ins do SnapCenter e credenciais adicionais para executar operações de proteção de dados em bancos de dados ou sistemas de arquivos do Windows.

Sobre esta tarefa

- Hosts Linux

  Você deve configurar credenciais para instalar plug-ins em hosts Linux.

Você deve configurar as credenciais para o usuário root ou para um usuário não root que tenha privilégios sudo para instalar e iniciar o processo do plug-in.

Melhores práticas: embora você tenha permissão para criar credenciais para o Linux após implantar hosts e instalar plug-ins, a melhor prática é criar credenciais depois de adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

  Você deve configurar as credenciais do Windows antes de instalar plug-ins.

  Você deve configurar as credenciais com privilégios de administrador, incluindo direitos de administrador no host remoto.

Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver privilégios de administrador completos, será necessário atribuir pelo menos os privilégios de grupo de recursos e backup ao nome de usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.
4. Na página Credencial, especifique as informações necessárias para configurar as credenciais:

Para este campo…	**Faça isso…**
Nome da credencial	Digite um nome para as credenciais.

Para este campo…	Faça isso…
Nome de usuário	Digite o nome de usuário e a senha que serão usados para autenticação. • Administrador de domínio ou qualquer membro do grupo de administradores Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS\Nome do Usuário* ◦ *FQDN do domínio\Nome do usuário* • Administrador local (somente para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é: *UserName* Não use aspas duplas (") ou acento grave (`) nas senhas. Você não deve usar os símbolos de menor que (<) e exclamação (!) juntos em senhas. Por exemplo, menor que <! 10, menor que 10 <!, acento grave `12.
Senha	Digite a senha usada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que você deseja usar.
Use privilégios sudo	Marque a caixa de seleção **Usar privilégios sudo** se estiver criando credenciais para um usuário não root. Aplicável somente a usuários do Linux.

5. Clique em **OK**.

Depois de concluir a configuração das credenciais, talvez você queira atribuir a manutenção de credenciais a um usuário ou grupo de usuários na página Usuário e Acesso.

Instalar o plug-in SnapCenter para MySQL

Adicionar hosts e instalar pacotes de plug-ins em hosts remotos

Você deve usar a página Adicionar Host do SnapCenter para adicionar hosts e, em seguida, instalar os pacotes de plug-ins. Os plug-ins são instalados automaticamente nos hosts remotos. Você pode adicionar o host e instalar pacotes de plug-in para um host individual.

Antes de começar

- Se o sistema operacional do host do SnapCenter Server for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deverá executar o seguinte:
  - Atualize para o Windows Server 2019 (versão do sistema operacional 17763.5936) ou posterior
  - Atualize para o Windows Server 2022 (versão do sistema operacional 20348.2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- A documentação de administração contém informações sobre o gerenciamento de hosts.

Sobre esta tarefa

- Não é possível adicionar um SnapCenter Server como um host de plug-in a outro SnapCenter Server.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Clique em **Adicionar**.
4. Na página Hosts, execute as seguintes ações:

Para este campo…	Faça isso…
Tipo de host	Selecione o tipo de host: • Windows • Linux O Plug-in para MySQL deve ser instalado no servidor de banco de dados MySQL.

Para este campo…	Faça isso…
Nome do host	Digite o nome do host de comunicação. Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o FQDN.
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais. Você pode visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial fornecida. O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar Host.

5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a serem instalados.

   Ao usar a API REST para instalar o Plug-in para MySQL, você deve passar a versão como 3.0. Por exemplo, MySQL:3.0

6. (Opcional) Clique em **Mais opções**.

Para este campo…	Faça isso…
Porta	Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.

Para este campo…	Faça isso…
Caminho de instalação	O Plug-in para MySQL é instalado no host do cliente MySQL, e esse host pode estar em um sistema Windows ou Linux. • Para o pacote de plug-ins SnapCenter para Windows, o caminho padrão é C:\Arquivos de Programas\ NetApp\ SnapCenter. Opcionalmente, você pode personalizar o caminho. • Para o pacote de plug-ins SnapCenter para Linux, o caminho padrão é /opt/ NetApp/snapcenter. Opcionalmente, você pode personalizar o caminho.
Ignorar verificações de pré-instalação	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.
Adicionar todos os hosts no cluster	Não aplicável.
Use a conta de serviço gerenciada em grupo (gMSA) para executar os serviços do plug-in	Não aplicável.

7. Clique em **Enviar**.

   Se você não tiver marcado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se ele atende aos requisitos para a instalação do plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão do .NET, a localização (para plug-ins do Windows) e a versão do Java (para plug-ins do Linux) são validados em relação aos requisitos mínimos. Se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas serão exibidas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em C:\Arquivos de Programas\ NetApp\ SnapCenter WebApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, deverá atualizar o arquivo em ambos os nós.

8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirmar e Enviar**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós do cluster.

   A verificação de impressão digital é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitore o progresso da instalação.
   - Para o plug-in do Windows, os logs de instalação e atualização estão localizados em: *C:\Windows\ SnapCenter plugin\Install*<JOBID>_

◦ Para o plug-in Linux, os logs de instalação estão localizados em: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log_ e os logs de atualização estão localizados em: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log_

Depois que você terminar

Se você quiser atualizar para a versão SnapCenter 6.0, o Plug-in baseado em PERL existente para MySQL será desinstalado do servidor de plug-in remoto.

Instalar pacotes de plug-in SnapCenter para Linux ou Windows em vários hosts remotos usando cmdlets

Você pode instalar os pacotes de plug-in do SnapCenter para Linux ou Windows em vários hosts simultaneamente usando o cmdlet Install-SmHostPackage do PowerShell.

Antes de começar

Você deve ter efetuado login no SnapCenter como um usuário de domínio com direitos de administrador local em cada host no qual deseja instalar o pacote de plug-in.

Passos

1. Inicie o PowerShell.
2. No host do SnapCenter Server, estabeleça uma sessão usando o cmdlet Open-SmConnection e insira suas credenciais.
3. Instale o plug-in em vários hosts usando o cmdlet Install-SmHostPackage e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

   Você pode usar a opção -skipprecheck quando tiver instalado os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

4. Insira suas credenciais para instalação remota.

Instale o plug-in SnapCenter para MySQL em hosts Linux usando a interface de linha de comando

Você deve instalar o plug-in SnapCenter para banco de dados MySQL usando a interface de usuário (IU) do SnapCenter . Se o seu ambiente não permitir a instalação remota do plug-in pela interface do usuário do SnapCenter , você poderá instalar o plug-in para o banco de dados MySQL no modo de console ou no modo silencioso usando a interface de linha de comando (CLI).

Antes de começar

- Você deve instalar o Plug-in para Banco de Dados MySQL em cada host Linux onde a instância do MySQL deve ser protegida.
- O host Linux no qual você está instalando o SnapCenter Plug-in para Banco de Dados MySQL deve atender aos requisitos de software, banco de dados e sistema operacional dependentes.

  A Ferramenta de Matriz de Interoperabilidade (IMT) contém as informações mais recentes sobre as configurações suportadas.

"Ferramenta de Matriz de Interoperabilidade da NetApp"

- O plug-in SnapCenter para banco de dados MySQL faz parte do pacote de plug-ins SnapCenter para Linux. Antes de instalar o SnapCenter Plug-ins Package para Linux, você já deve ter instalado o SnapCenter em um host Windows.

Passos

1. Copie o arquivo de instalação do pacote de plug-ins SnapCenter para Linux (snapcenter_linux_host_plugin.bin) de C:\ProgramData\ NetApp\ SnapCenter\Package Repository para o host onde você deseja instalar o plug-in para MySQL.

   Você pode acessar esse caminho a partir do host onde o SnapCenter Server está instalado.

2. No prompt de comando, navegue até o diretório onde você copiou o arquivo de instalação.
3. Instale o plug-in: `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 especifica a porta de comunicação HTTPS do SMCore.
   - -DSERVER_IP especifica o endereço IP do SnapCenter Server.
   - -DSERVER_HTTPS_PORT especifica a porta HTTPS do SnapCenter Server.
   - -DUSER_INSTALL_DIR especifica o diretório onde você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
   - DINSTALL_LOG_NAME especifica o nome do arquivo de log.

   ```
   /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. Edite o arquivo /<diretório de instalação>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties e adicione o parâmetro PLUGINS_ENABLED = MySQL:3.0.
5. Adicione o host ao SnapCenter Server usando o cmdlet Add-Smhost e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitore o status da instalação do Plug-in para MySQL

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
   a. Clique em **Filtrar**.
   b. Opcional: especifique a data de início e término.
   c. No menu suspenso Tipo, selecione **Instalação de plug-in**.
   d. No menu suspenso Status, selecione o status da instalação.
   e. Clique em **Aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Configurar certificado CA

Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.

O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte "Como gerar um arquivo CSR de certificado CA" .

Se você possui o certificado CA para seu domínio (*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Importar chave privada	Selecione a opção **Sim**, importe a chave privada e clique em **Avançar**.
Formato de arquivo de importação	Não faça alterações; clique em **Avançar**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

> O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: *.pfx, *.p12 e *.p7b).

7. Repita a Etapa 5 para a pasta “Pessoal”.

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

Passos

1. Execute o seguinte na GUI:
   a. Clique duas vezes no certificado.
   b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.
   c. Percorra a lista de campos e clique em **Impressão digital**.
   d. Copie os caracteres hexadecimais da caixa.

e. Remova os espaços entre os números hexadecimais.

   Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:
   a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

      Get-ChildItem -Path Cert:\LocalMachine\My

   b. Copie a impressão digital.

Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Por exemplo:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Vincule o certificado recém-instalado aos serviços de plug-in do host do Windows, executando os seguintes comandos:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

   Por exemplo:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert appid="$guid"
   ```

Configurar o certificado CA para o serviço SnapCenter MySQL Plug-ins no host Linux

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo 'keystore.jks', que está localizado em */opt/ NetApp/snapcenter/scc/etc* como seu armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in a partir do arquivo de propriedades do agente do plug-in.

   É o valor correspondente à chave 'KEYSTORE_PASS'.

2. Alterar a senha do keystore:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Altere a senha de todos os aliases de entradas de chave privada no
   keystore para a mesma senha usada para o keystore:
   ```

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

3. Reinicie o serviço após alterar a senha.

> A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Adicione um certificado raiz ou intermediário:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Reinicie o serviço após configurar os certificados raiz ou
intermediários para conectar o trust-store.
```

Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Adicione o certificado da CA com chave privada e pública.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Listar os certificados adicionados no keystore.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

   A senha padrão do keystore do plug-in é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Se o nome do alias no certificado da CA for longo e contiver espaços
   ou caracteres especiais ("*",","), altere o nome do alias para um nome
   simples:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configure o nome do alias do certificado CA no arquivo
   agent.properties.
   ```

   Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

Configurar lista de revogação de certificados (CRL) para plug-ins

Sobre esta tarefa

- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é ' opt/NetApp/snapcenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties em relação à chave CRL_PATH.

   Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Configurar o certificado CA para o serviço SnapCenter MySQL Plug-ins no host Windows

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo *keystore.jks*, que está localizado em *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* como seu armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in a partir do arquivo de propriedades do agente do plug-in.

   É o valor correspondente à chave *KEYSTORE_PASS*.

2. Alterar a senha do keystore:

   keytool -storepasswd -keystore keystore.jks

   > Se o comando "keytool" não for reconhecido no prompt de comando do Windows, substitua o comando keytool pelo seu caminho completo.

   C:\Arquivos de Programas\Java\<versão_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. Altere a senha de todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:

   keytool -keypasswd -alias "nome_do_alias_no_certificado" -keystore keystore.jks

   Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

4. Reinicie o serviço após alterar a senha.

A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

   keytool -list -v -keystore keystore.jks

4. Adicione um certificado raiz ou intermediário:

   keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Reinicie o serviço após configurar os certificados raiz ou intermediários para conectar o trust-store.

Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo *keystore.jks*.
3. Listar os certificados adicionados no keystore:

   keytool -list -v -keystore keystore.jks

4. Adicione o certificado da CA com chave privada e pública.

   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS

5. Listar os certificados adicionados no keystore.

   keytool -list -v -keystore keystore.jks

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

   A senha padrão do keystore do plug-in é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

   keytool -keypasswd -alias "nome_do_alias_no_certificado_da_CA" -keystore keystore.jks

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

   Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

Configurar lista de revogação de certificados (CRL) para plug-ins SnapCenter

Sobre esta tarefa

- Para baixar o arquivo CRL mais recente para o certificado CA relacionado, consulte "Como atualizar o arquivo de lista de revogação de certificados no SnapCenter CA Certificate" .
- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é *'C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo *agent.properties* em relação à chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

   Os certificados recebidos serão verificados em relação a cada CRL.

Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *Get-SmCertificateSettings*.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- * 🔒 * indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.

- * * indica que o certificado CA foi validado com sucesso.
- * * indica que o certificado CA não pôde ser validado.
- * * indica que as informações de conexão não puderam ser recuperadas.

Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Prepare-se para a proteção de dados

Pré-requisitos para usar o plug-in SnapCenter para MySQL

Antes de usar o SnapCenter Plug-in para MySQL, o administrador do SnapCenter deve instalar e configurar o SnapCenter Server e executar as tarefas de pré-requisito.

- Instalar e configurar o SnapCenter Server.
- Efetue login no SnapCenter Server.
- Configure o ambiente SnapCenter adicionando conexões do sistema de armazenamento e criando credenciais, se aplicável.
- Instale o Java 11 no seu host Linux ou Windows.

  Você deve definir o caminho Java na variável de caminho ambiental da máquina host.

- Configure o SnapMirror e o SnapVault se desejar replicação de backup.

Como recursos, grupos de recursos e políticas são usados para proteger o MySQL

Antes de usar o SnapCenter, é útil entender os conceitos básicos relacionados às operações de backup, clonagem e restauração que você deseja executar. Você interage com recursos, grupos de recursos e políticas para diferentes operações.

- Os recursos geralmente são instâncias do MySQL que você faz backup ou clona com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host.

  Ao executar uma operação em um grupo de recursos, você executa essa operação nos recursos definidos no grupo de recursos de acordo com o cronograma especificado para o grupo de recursos.

  Você pode fazer backup sob demanda de um único recurso ou de um grupo de recursos. Você também pode executar backups agendados para recursos individuais e grupos de recursos.

- As políticas especificam a frequência de backup, replicação, scripts e outras características das operações de proteção de dados.

  Ao criar um grupo de recursos, você seleciona uma ou mais políticas para esse grupo. Você também pode selecionar uma política ao executar um backup sob demanda para um único recurso.

Pense em um grupo de recursos como algo que define o que você quer proteger e quando quer proteger em termos de dia e hora. Pense em uma política como a definição de como você deseja protegê-la. Se você estiver fazendo backup de todos os bancos de dados, por exemplo, poderá criar um grupo de recursos que

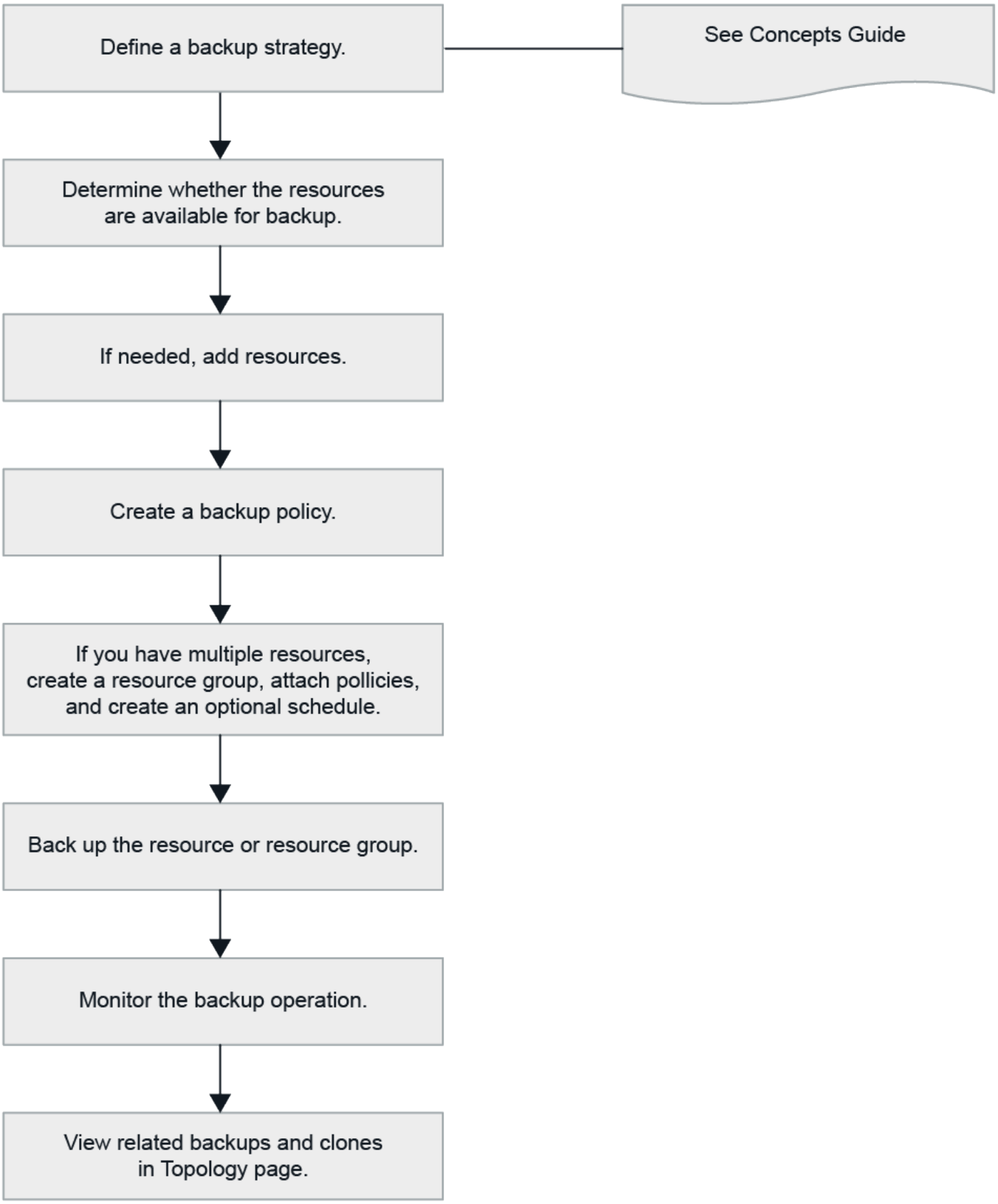
inclua todos os bancos de dados no host. Você pode então anexar duas políticas ao grupo de recursos: uma política diária e uma política horária. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diariamente.

Fazer backup dos recursos do MySQL

Fazer backup dos recursos do MySQL

Você pode criar um backup de um recurso (banco de dados) ou grupo de recursos. O fluxo de trabalho de backup inclui planejamento, identificação dos bancos de dados para backup, gerenciamento de políticas de backup, criação de grupos de recursos e anexação de políticas, criação de backups e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de backup:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell. "Guia de referência do cmdlet do software SnapCenter" .

Descubra os bancos de dados automaticamente

Os recursos são bancos de dados MySQL no host Linux que são gerenciados pelo SnapCenter. Você pode adicionar os recursos aos grupos de recursos para executar operações de proteção de dados depois de descobrir os bancos de dados MySQL disponíveis.

Antes de começar

- Você já deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts e configurar as conexões do sistema de armazenamento.
- O plug-in SnapCenter para MySQL não oferece suporte à descoberta automática de recursos que residem em ambientes virtuais RDM/VMDK. Você deve fornecer as informações de armazenamento para ambientes virtuais ao adicionar os bancos de dados manualmente.

Sobre esta tarefa

- Após instalar o plug-in, todos os bancos de dados naquele host Linux são descobertos automaticamente e exibidos na página Recursos.
- Somente bancos de dados são descobertos automaticamente.

Os recursos descobertos automaticamente não podem ser modificados ou excluídos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o Plug-in para MySQL na lista.
2. Na página Recursos, selecione o tipo de recurso na lista Exibir.
3. (Opcional) Clique em * * e, em seguida, selecione o nome do host.

   Você pode então clicar em * * para fechar o painel de filtro.

4. Clique em **Atualizar recursos** para descobrir os recursos disponíveis no host.

   Os recursos são exibidos junto com informações como tipo de recurso, nome do host, grupos de recursos associados, tipo de backup, políticas e status geral.

   - Se o banco de dados estiver em um armazenamento NetApp e não estiver protegido, Não protegido será exibido na coluna Status geral.
   - Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, e se nenhuma operação de backup for realizada, Backup não executado será exibido na coluna Status geral. Caso contrário, o status mudará para Falha no backup ou Backup bem-sucedido com base no último status do backup.

Você deve atualizar os recursos se as instâncias forem renomeadas fora do SnapCenter.

Adicionar recursos manualmente ao host do plug-in

A descoberta automática não é suportada no host Windows. Você deve adicionar instâncias do MySQL e recursos de banco de dados manualmente.

Antes de começar

- Você deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts e configurar conexões do sistema de armazenamento.

Passos

1. No painel de navegação esquerdo, selecione o SnapCenter Plug-in para MySQL na lista suspensa e clique em **Recursos**.
2. Na página Recursos, clique em **Adicionar recursos do MySQL**.
3. Na página Fornecer detalhes do recurso, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Especifique o nome do banco de dados.
Nome do host	Digite o nome do host.
Tipo	Selecione a instância.
Exemplo	Não aplicável.
Credenciais	Selecione as credenciais ou adicione informações para a credencial. Isto é opcional.

4. Na página Fornecer espaço de armazenamento, selecione um tipo de armazenamento e escolha um ou mais volumes, LUNs e qtrees e clique em **Salvar**.

   Opcional: Você pode clicar no * + * ícone para adicionar mais volumes, LUNs e qtrees de outros sistemas de armazenamento.

5. Opcional: Na página Configurações de recursos, insira pares de chave-valor personalizados para o plug-in MySQL.
6. Revise o resumo e clique em **Concluir**.

   Os bancos de dados são exibidos junto com informações como o nome do host, grupos de recursos e políticas associados e status geral

Se você quiser fornecer aos usuários acesso aos recursos, deverá atribuir os recursos aos usuários. Isso permite que os usuários executem as ações para as quais têm permissão nos ativos atribuídos a eles.

"Adicionar um usuário ou grupo e atribuir função e ativos"

Depois de adicionar os bancos de dados, você pode modificar os detalhes do banco de dados MySQL.

Criar políticas de backup para MySQL

Antes de usar o SnapCenter para fazer backup de recursos do MySQL, você deve criar uma política de backup para o recurso ou grupo de recursos que deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e mantém backups.

Antes de começar

- Você deve ter definido sua estratégia de backup.

  Para obter detalhes, consulte as informações sobre como definir uma estratégia de proteção de dados para bancos de dados MySQL.

- Você deve ter se preparado para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, configurar conexões do sistema de armazenamento e adicionar recursos.
- O administrador do SnapCenter deve ter atribuído as SVMs para os volumes de origem e destino a você se estiver replicando instantâneos para um espelho ou cofre.

  Além disso, você pode especificar configurações de replicação, script e aplicativo na política. Essas opções economizam tempo quando você deseja reutilizar a política para outro grupo de recursos.

Sobre esta tarefa

- SnapLock
  - Se a opção 'Manter as cópias de backup por um número específico de dias' for selecionada, o período de retenção do SnapLock deverá ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio de instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar à retenção de um número maior de instantâneos do que a contagem especificada na política.
  - Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Clique em **Novo**.
4. Na página Nome, insira o nome e os detalhes da política.
5. Na página Tipo de política, faça o seguinte:
   a. Selecione o tipo de armazenamento.
   b. Na seção Configurações de backup personalizadas, forneça quaisquer configurações de backup específicas que devem ser passadas ao plug-in no formato chave-valor.

      Você pode fornecer vários valores-chave a serem passados ao plug-in.

6. Na página Snapshot e Replicação, execute as seguintes etapas:
   a. Especifique o tipo de programação selecionando **Sob demanda**, **Por hora**, **Diário**, **Semanal** ou **Mensal**.

      Você pode especificar o agendamento (data de início, data de término e frequência) para a operação de backup ao criar um grupo de recursos. Isso permite que você crie grupos de recursos que compartilham a mesma política e frequência de backup, mas permite que você atribua agendamentos de backup diferentes a cada política.

Se você agendou para 2h00, a programação não será acionada durante o horário de verão (DST).

a. Na seção Configurações de instantâneo, especifique as configurações de retenção para o tipo de backup e o tipo de agendamento selecionado na página **Tipo de backup**:

Se você quiser…	Então…
Mantenha um certo número de Snapshots	Selecione **Cópias a serem mantidas** e especifique o número de Snapshots que você deseja manter. Se o número de Snapshots exceder o número especificado, os Snapshots serão excluídos, com as cópias mais antigas sendo excluídas primeiro. Você deve definir a contagem de retenção como 2 ou mais se planeja habilitar a replicação do SnapVault . Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro Snapshot será o Snapshot de referência para o relacionamento SnapVault até que um Snapshot mais recente seja replicado para o destino. O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida como um valor maior do que o suportado pela versão subjacente do ONTAP .
Mantenha os Snapshots por um certo número de dias	Selecione **Manter cópias por** e especifique o número de dias pelos quais você deseja manter os Snapshots antes de excluí-los.
Período de bloqueio de cópia de instantâneo	Selecione **Período de bloqueio de cópia de instantâneo** e especifique dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

b. Selecione um rótulo de política.

Você pode atribuir rótulos SnapMirror a snapshots primários para replicação remota, permitindo que os snapshots primários descarreguem a operação de replicação de snapshots do SnapCenter para sistemas secundários ONTAP . Isso pode ser feito sem habilitar a opção SnapMirror ou SnapVault na página de política.

7. Na seção Selecionar opções de replicação secundária, selecione uma ou ambas as seguintes opções de replicação secundária:

Para este campo…	Faça isso…
Atualize o SnapMirror após criar uma cópia local do Snapshot	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Se o relacionamento de proteção no ONTAP for do tipo Mirror and Vault e se você selecionar apenas esta opção, o Snapshot criado no primário não será transferido para o destino, mas será listado no destino. Se este Snapshot for selecionado no destino para executar uma operação de restauração, a seguinte mensagem de erro será exibida: O local secundário não está disponível para o backup em cofre/espelho selecionado. Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Ver "Visualize backups e clones relacionados a recursos do MySQL na página Topologia" .
Atualize o SnapVault após criar uma cópia local do Snapshot	Selecione esta opção para executar a replicação de backup de disco para disco (backups do SnapVault). Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Quando o SnapLock é configurado somente no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página Topologia atualiza o período de bloqueio no secundário recuperado do ONTAP. Para obter mais informações sobre o SnapLock Vault, consulte Confirmar instantâneos para WORM em um destino de cofre Ver "Visualize backups e clones relacionados a recursos do MySQL na página Topologia" .

Para este campo…	Faça isso…
Erro na contagem de novas tentativas	Insira o número máximo de tentativas de replicação que podem ser permitidas antes que a operação seja interrompida.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o armazenamento secundário para evitar atingir o limite máximo de Snapshots no armazenamento secundário.

8. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas

Um grupo de recursos é o contêiner ao qual você deve adicionar recursos que deseja fazer backup e proteger. Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente. Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que deseja executar.

Sobre esta tarefa

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Insira um nome para o grupo de recursos. O nome do grupo de recursos não deve exceder 250 caracteres.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.

Para este campo…	Faça isso…
Use formato de nome personalizado para cópia de instantâneo	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do instantâneo. Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do instantâneo.

4. Na página Recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Tipo de recurso**.

   Isso ajuda a filtrar informações na tela.

5. Selecione os recursos na seção **Recursos disponíveis** e clique na seta para a direita para movê-los para a seção **Recursos selecionados**.
6. Na página Configurações do aplicativo, faça o seguinte:

   a. Clique na seta **Backups** para definir opções adicionais de backup:

      Habilite o backup do grupo de consistência e execute as seguintes tarefas:

Para este campo…	Faça isso…
Permitir tempo para esperar a conclusão da operação de instantâneo do Consistency Group	Selecione **Urgente**, **Médio** ou **Relaxado** para especificar o tempo de espera para a conclusão da operação de instantâneo. Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.
Desativar sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL .

+

a. Clique na seta **Scripts** e insira os comandos pre e post para operações de inatividade, snapshot e unquiesce. Você também pode inserir os pré-comandos a serem executados antes de sair em caso de falha.

b. Clique na seta **Configurações personalizadas** e insira os pares de chave-valor personalizados necessários para todas as operações de proteção de dados que usam este recurso.

Parâmetro	Contexto	Descrição
HABILITAR_REGISTRO_DE_ARQUIVO	(S/N)	Permite que o gerenciamento de log de arquivamento exclua os logs de arquivamento.
RETENÇÃO_DE_REGISTRO_DE_ARQUIVO	número_de_dias	Especifica o número de dias que os logs de arquivamento são retidos. Esta configuração deve ser igual ou maior que NTAP_SNAPSHOT_RETENTIONS.
DIRETÓRIO_DE_LOG_DE_ARQUIVO	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs de arquivamento.

Parâmetro	Contexto	Descrição
EXT_DE_LOG_DE_ARQUIVO	extensão_de_arquivo	Especifica o comprimento da extensão do arquivo de log de arquivamento. Por exemplo, se o log de arquivamento for log_backup_0_0_0_0.16151855 1942 9 e se o valor file_extension for 5, a extensão do log manterá 5 dígitos, que é 16151.
ARQUIVO_LOG_RECURSIVO_ SE ARQUIVO	(S/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs de arquivamento estiverem localizados em subdiretórios.

Os pares de chave-valor personalizados são suportados por sistemas de plug-in MySQL Linux e não são suportados por bancos de dados MySQL registrados como um plug-in centralizado do Windows.

c. Clique na seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar instantâneos:

Se você quiser…	Então…
SnapCenter para usar o plug-in para Windows e colocar o sistema de arquivos em um estado consistente antes de criar um snapshot. Para recursos do Linux, esta opção não é aplicável.	Selecione * SnapCenter com consistência do sistema de arquivos*.
SnapCenter para criar um instantâneo de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.
Para inserir o comando a ser executado no host para criar cópias de instantâneos.	Selecione **Outro** e insira o comando a ser executado no host para criar um instantâneo.

7. Na página Políticas, execute as seguintes etapas:

a. Selecione uma ou mais políticas na lista suspensa.

Você também pode criar uma política clicando em * + *.

As políticas são listadas na seção Configurar agendamentos para políticas selecionadas.

b. Na coluna Configurar agendamentos, clique em * + * para a política que você deseja configurar.

c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

Onde policy_name é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna **Agendamentos Aplicados**.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. O servidor SMTP deve ser configurado em **Configurações** > **Configurações globais**.

9. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e habilite proteção secundária para recursos MySQL em sistemas ASA r2

Você deve criar o grupo de recursos para adicionar os recursos que estão nos sistemas ASA r2. Você também pode provisionar a proteção secundária ao criar o grupo de recursos.

Antes de começar

- Você deve garantir que não está adicionando recursos do ONTAP 9.x e recursos do ASA r2 ao mesmo grupo de recursos.
- Você deve garantir que não tenha um banco de dados com recursos ONTAP 9.x e recursos ASA r2.

Sobre esta tarefa

- A proteção secundária estará disponível somente se o usuário conectado estiver atribuído à função que tem o recurso **SecondaryProtection** habilitado.
- Se você habilitar a proteção secundária, o grupo de recursos será colocado no modo de manutenção durante a criação dos grupos de consistência primário e secundário. Depois que os grupos de consistência primário e secundário são criados, o grupo de recursos é retirado do modo de manutenção.
- O SnapCenter não oferece suporte à proteção secundária para um recurso clone.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:
   a. Insira um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 caracteres.

   b. Insira um ou mais rótulos no campo Tag para ajudar você a pesquisar o grupo de recursos posteriormente.

Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.

c. Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

d. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

Você deve usar exatamente o mesmo destino definido no aplicativo, incluindo o prefixo, se necessário.

4. Na página Recursos, selecione o nome do host do banco de dados na lista suspensa **Host**.

Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos do ASA r2 na seção Recursos disponíveis e mova-os para a seção Recursos selecionados.
6. Na página Configurações do aplicativo, selecione a opção de backup.
7. Na página Políticas, execute as seguintes etapas:

a. Selecione uma ou mais políticas na lista suspensa.

Você também pode criar uma política clicando em + .

Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

Onde *policy_name* é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Se a proteção secundária estiver habilitada para a política selecionada, a página Proteção Secundária será exibida e você precisará executar as seguintes etapas:

a. Selecione o tipo de política de replicação.

A política de replicação síncrona não é suportada.

b. Especifique o sufixo do grupo de consistência que você deseja usar.

c. Nos menus suspensos Cluster de destino e SVM de destino, selecione o cluster emparelhado e o SVM que você deseja usar.

> O cluster e o peering de SVM não são suportados pelo SnapCenter. Você deve usar o System Manager ou as CLIs do ONTAP para executar o peering de cluster e SVM.

> Se os recursos já estiverem protegidos fora do SnapCenter, eles serão exibidos na seção Recursos Protegidos Secundários.

1. Na página Verificação, execute as seguintes etapas:

   a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para realizar a verificação no armazenamento secundário.

   b. Clique + na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política.

   c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name, execute as seguintes ações:

Se você quiser…	Faça isso…
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

   d. Selecione **Verificar no local secundário** para verificar seus backups no sistema de armazenamento secundário.

   e. Clique em **OK**.

   Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

2. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

   > Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

3. Revise o resumo e clique em **Concluir**.

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para MySQL

Você deve criar uma conexão de máquina virtual de armazenamento (SVM) e uma

credencial antes de usar cmdlets do PowerShell para fazer backup, restaurar ou clonar bancos de dados MySQL.

Antes de começar

- Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.
- Você deve ter as permissões necessárias na função de administrador de infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estejam em andamento.

  As instalações do plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento porque o cache do host pode não ser atualizado e o status dos bancos de dados pode ser exibido na GUI do SnapCenter como “Não disponível para backup” ou "`Não no armazenamento NetApp ".

- Os nomes dos sistemas de armazenamento devem ser exclusivos.

  O SnapCenter não oferece suporte a vários sistemas de armazenamento com o mesmo nome em clusters diferentes. Cada sistema de armazenamento suportado pelo SnapCenter deve ter um nome exclusivo e um endereço IP LIF de dados exclusivo.

Passos

1. Inicie uma sessão de conexão do PowerShell Core usando o cmdlet Open-SmConnection.

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

2. Crie uma nova conexão com o sistema de armazenamento usando o cmdlet Add-SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Crie uma nova credencial usando o cmdlet Add-SmCredential.

   Este exemplo mostra como criar uma nova credencial chamada FinanceAdmin com credenciais do Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Adicione o host de comunicação MySQL ao SnapCenter Server.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode mysql
```

5. Instale o pacote e o plug-in SnapCenter para MySQL no host.

Para Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
mysql
```

Para Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode mysql
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. Defina o caminho para o SQLLIB.

   Para Windows, o plug-in MySQL usará o caminho padrão para a pasta SQLLIB: “C:\Arquivos de Programas\IBM\SQLLIB\BIN”

   Se você quiser substituir o caminho padrão, use o seguinte comando.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
MySQL -configSettings @{“MySQL_SQLLIB_CMD” =
“<custom_path>\IBM\SQLLIB\BIN”}
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup do MySQL

Se um recurso ainda não fizer parte de nenhum grupo de recursos, você poderá fazer backup do recurso na página Recursos.

Antes de começar

- Você deve ter criado uma política de backup.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.
- Para a operação de backup baseada em cópia de instantâneo, certifique-se de que todos os bancos de dados de locatários sejam válidos e ativos.
- Para comandos pré e pós para operações de inatividade, instantâneo e retomada de atividade, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recurso, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Selecione * * e selecione o nome do host e o tipo de recurso para filtrar os recursos. Você pode então selecionar para fechar o painel de filtro.
3. Selecione o recurso que você deseja fazer backup.
4. Na página Recurso, selecione **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.
5. Na página Configurações do aplicativo, faça o seguinte:
   - Selecione a seta **Backups** para definir opções adicionais de backup:

     Habilite o backup do grupo de consistência, se necessário, e execute as seguintes tarefas:

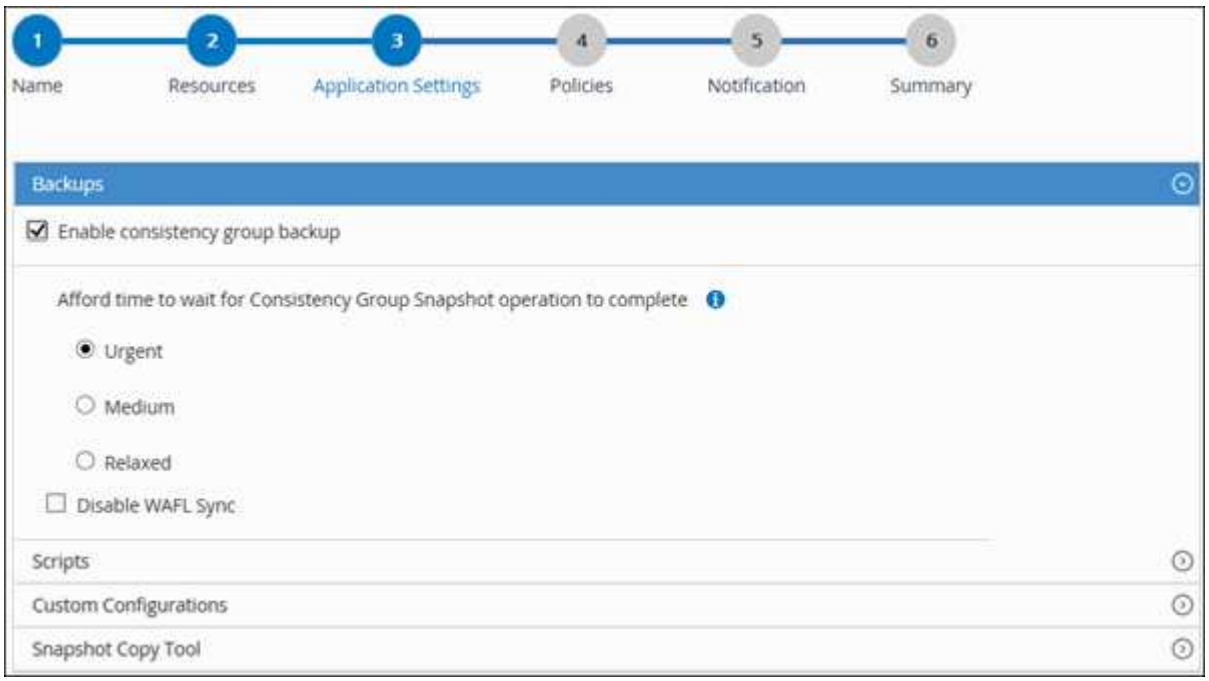
Para este campo…	Faça isso…
Permitir tempo para esperar a conclusão da operação "Consistency Group Snapshot"	Selecione **Urgente**, ou **Médio**, ou **Relaxado** para especificar o tempo de espera para a operação de Snapshot terminar. Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.
Desativar sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL .

   - Selecione a seta **Scripts** para executar comandos pré e pós para operações de inatividade, instantâneo e ativação/desativação.

     Você também pode executar pré-comandos antes de sair da operação de backup. Prescrições e pós-escritos são executados no SnapCenter Server.
   - Selecione a seta **Configurações personalizadas** e insira os pares de valores personalizados necessários para todos os trabalhos que usam este recurso.
   - Selecione a seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar Instantâneos:

Se você quiser…	Então…
SnapCenter para criar um Snapshot de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.

Se você quiser…	Então…
SnapCenter para usar o plug-in para Windows para colocar o sistema de arquivos em um estado consistente e, em seguida, criar um Snapshot	Selecione * SnapCenter com consistência do sistema de arquivos*.
Para inserir o comando para criar um Snapshot	Selecione **Outro** e insira o comando para criar um Snapshot.



6. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em * + *.

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Selecione * + * na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

   c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione **OK**.

      policy_name é o nome da política que você selecionou.

   Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

7. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. O SMTP também deve ser configurado em **Configurações** > **Configurações globais**.

8. Revise o resumo e selecione **Concluir**.

   A página de topologia de recursos é exibida.

9. Selecione **Fazer backup agora**.
10. Na página Backup, execute as seguintes etapas:
    a. Se você aplicou várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

       Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

    b. Selecione **Backup**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.
    - Nas configurações do MetroCluster , o SnapCenter pode não conseguir detectar um relacionamento de proteção após um failover.

      Para mais informações, consulte: "Não é possível detectar o relacionamento SnapMirror ou SnapVault após failover do MetroCluster"

    - Se você estiver fazendo backup de dados do aplicativo em VMDKs e o tamanho do heap Java para o SnapCenter Plug-in for VMware vSphere não for grande o suficiente, o backup poderá falhar.

      Para aumentar o tamanho do heap Java, localize o arquivo de script */opt/netapp/init_scripts/scvservice*. Nesse script, o comando *do_start method* inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: *Java -jar -Xmx8192M -Xms4096M*

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

   ```
   Open-SmConnection  -SMSbaseurl
   https:\\snapctr.demo.netapp.com:8146\
   ```

   O prompt de nome de usuário e senha é exibido.

2. Adicione recursos manuais usando o cmdlet Add-SmResources.

   Este exemplo mostra como adicionar uma instância do MySQL:

```
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. Crie uma política de backup usando o cmdlet Add-SmPolicy.
4. Proteja o recurso ou adicione um novo grupo de recursos ao SnapCenter usando o cmdlet Add-SmResourceGroup.
5. Inicie uma nova tarefa de backup usando o cmdlet New-SmBackup.

   Este exemplo mostra como fazer backup de um grupo de recursos:

   ```
   C:\PS> New-SmBackup -Resources
   @{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306";"P
   luginName"="MySQL"} -Policy "MySQL_snapshotbased"
   ```

   Este exemplo faz backup de um recurso protegido:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
   -Policy mysql_policy2
   ```

6. Monitore o status do trabalho (em execução, concluído ou com falha) usando o cmdlet Get-smJobSummaryReport.

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. Monitore os detalhes do trabalho de backup, como ID do backup, nome do backup para executar a operação de restauração ou clonagem usando o cmdlet Get-SmBackupReport.

```
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 :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Fazer backup de grupos de recursos

Um grupo de recursos é uma coleção de recursos em um host. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos.

Antes de começar

- Você deve ter criado um grupo de recursos com uma política anexada.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.

Sobre esta tarefa

Você pode fazer backup de um grupo de recursos sob demanda na página Recursos. Se um grupo de recursos tiver uma política anexada e um agendamento configurado, os backups ocorrerão automaticamente de acordo com o agendamento.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.

   Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou selecionando e, em seguida, selecionando a tag. Você pode então selecionar para fechar o painel de filtro.

3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e selecione **Fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
   a. Se você associou várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

      Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

   b. Selecione **Backup**.
5. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Monitorar operações de backup do MySQL

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Talvez você queira verificar o progresso para determinar quando ele foi concluído ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado correspondente das operações:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **Trabalhos**.
3. Na página Trabalhos, execute as seguintes etapas:

a. Clique para filtrar a lista de modo que somente as operações de backup sejam listadas.
b. Especifique as datas de início e término.
c. Na lista suspensa **Tipo**, selecione **Backup**.
d. No menu suspenso **Status**, selecione o status do backup.
e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.

4. Selecione uma tarefa de backup e clique em **Detalhes** para visualizar os detalhes da tarefa.

> Embora o status do trabalho de backup seja exibido , ao clicar em detalhes do trabalho, você poderá ver que algumas das tarefas filhas da operação de backup ainda estão em andamento ou marcadas com sinais de alerta.

5. Na página Detalhes do trabalho, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Monitore as operações de proteção de dados em instâncias do MySQL no painel Atividade

O painel Atividade exibe as cinco operações mais recentes realizadas. O painel Atividade também exibe quando a operação foi iniciada e o status da operação.

O painel Atividade exibe informações sobre operações de backup, restauração, clonagem e backup agendado.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Clique no painel Atividade para visualizar as cinco operações mais recentes.

   Quando você clica em uma das operações, os detalhes da operação são listados na página **Detalhes do trabalho**.

Cancelar operações de backup para MySQL

Você pode cancelar operações de backup que estão na fila.

O que você vai precisar

- Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de backup em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** fica desabilitado para operações que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de backup enfileiradas de outros membros enquanto estiver usando essa função.

Passos

1. Execute uma das seguintes ações:

Do…	Ação
Página do monitor	a. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. b. Selecione a operação e clique em **Cancelar trabalho**.
Painel de atividades	a. Após iniciar a operação de backup, clique em * * no painel Atividade para visualizar as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

A operação é cancelada e o recurso é revertido ao estado anterior.

Visualize backups e clones do MySQL na página Topologia

Ao se preparar para fazer backup ou clonar um recurso, pode ser útil visualizar uma representação gráfica de todos os backups e clones no armazenamento primário e secundário.

Sobre esta tarefa

Você pode revisar os seguintes ícones na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no armazenamento primário ou secundário (cópias espelhadas ou cópias do Vault).

-  exibe o número de backups e clones que estão disponíveis no armazenamento primário.
-  exibe o número de backups e clones que são espelhados no armazenamento secundário usando a tecnologia SnapMirror .
-  exibe o número de backups e clones que são replicados no armazenamento secundário usando a tecnologia SnapVault .

O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou 6 backups usando uma política para manter apenas 4 backups, o número de backups exibidos será 6.

Clones de um backup de um espelho flexível em termos de versão em um volume do tipo mirror-vault são exibidos na exibição de topologia, mas a contagem de backups de espelho na exibição de topologia não inclui o backup flexível em termos de versão.

Na página Topologia, você pode ver todos os backups e clones disponíveis para o recurso ou grupo de recursos selecionado. Você pode visualizar os detalhes desses backups e clones e selecioná-los para executar operações de proteção de dados.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso na exibição de detalhes do recurso ou na exibição de detalhes do grupo de recursos.

   Se o recurso estiver protegido, a página de topologia do recurso selecionado será exibida.

4. Revise o **cartão Resumo** para ver um resumo do número de backups e clones disponíveis no armazenamento primário e secundário.

   A seção **Cartão de resumo** exibe o número total de backups baseados em cópias de instantâneo e clones.

   Clicar no botão **Atualizar** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clicar no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Uma programação semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo estiver distribuído em vários volumes, o tempo de expiração do SnapLock para o backup será o maior tempo de expiração do SnapLock definido para um Snapshot em um volume. O maior tempo de expiração do SnapLock é recuperado do ONTAP.

   Após o backup sob demanda, clicar no botão **Atualizar** atualiza os detalhes do backup ou clone.

5. Na exibição Gerenciar cópias, clique em **Backups** ou **Clones** do armazenamento primário ou secundário para ver detalhes de um backup ou clone.

   Os detalhes dos backups e clones são exibidos em formato de tabela.

6. Selecione o backup na tabela e clique nos ícones de proteção de dados para executar operações de restauração, clonagem e exclusão.

   Não é possível renomear ou excluir backups que estejam no armazenamento secundário.

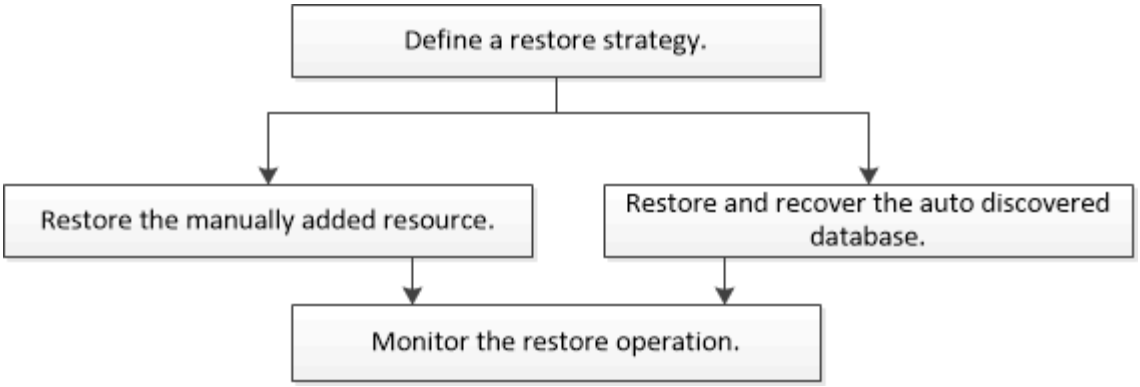
7. Se você quiser excluir um clone, selecione o clone na tabela e clique em .
8. Se você quiser dividir um clone, selecione o clone na tabela e clique em .

Restaurar MySQL

Fluxo de trabalho de restauração

O fluxo de trabalho de restauração e recuperação inclui planejamento, execução de operações de restauração e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de restauração:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre os cmdlets do PowerShell.

"Guia de referência do cmdlet do software SnapCenter" .

Restaurar e recuperar um backup de recurso adicionado manualmente

Você pode usar o SnapCenter para restaurar e recuperar dados de um ou mais backups.

Antes de começar

- Você deve ter feito backup do recurso ou dos grupos de recursos.
- Você deve ter cancelado qualquer operação de backup que esteja em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos de pré-restauração, pós-restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos Snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com o tipo, host, grupos de recursos e políticas associados e status.

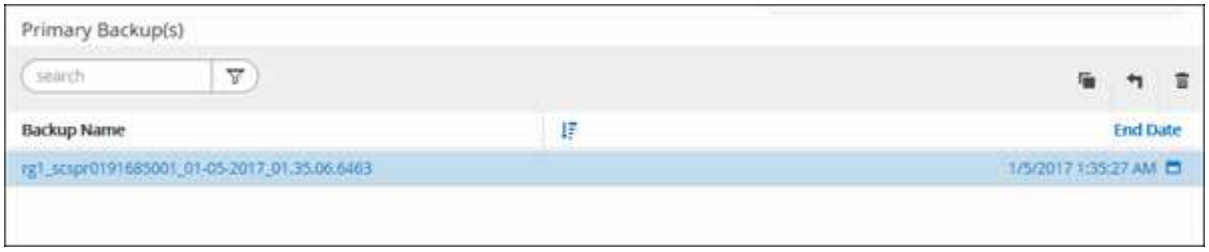
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, “Não protegido” será exibido na coluna Status geral. Isso pode significar que o recurso não está protegido ou que o backup do recurso foi feito por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e depois selecione um recurso nesse grupo.

   A página de topologia de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela Backup(s) primário(s), selecione o backup que deseja restaurar e clique em * * .



6. Na página Escopo de restauração, selecione **Recurso completo**.

   a. Se você selecionar **Recurso Completo**, todos os volumes de dados configurados do banco de dados MySQL serão restaurados.

      Se o recurso contiver volumes ou qtrees, os Snapshots tirados após o Snapshot selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

      Você pode selecionar vários LUNs.

      Se você selecionar **Todos**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.

7. Na página Pré-operações, insira os comandos pre restore e unmount para executar antes de realizar um trabalho de restauração.

   Os comandos de desmontagem não estão disponíveis para recursos descobertos automaticamente.

8. Na página Post ops, insira os comandos mount e post restore para serem executados após realizar

um trabalho de restauração.

Os comandos de montagem não estão disponíveis para recursos descobertos automaticamente.

9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O SMTP também deve ser configurado na página **Configurações** > **Configurações globais**.

10. Revise o resumo e clique em **Concluir**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
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
```

   Este exemplo exibe informações detalhadas sobre o backup de 29 de janeiro de 2015 a 3 de fevereiro de 2015:

```
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. Restaure os dados do backup usando o cmdlet Restore-SmBackup.

```
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          :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Restaurar e recuperar um backup de banco de dados descoberto automaticamente

Você pode usar o SnapCenter para restaurar e recuperar dados de um ou mais backups.

Antes de começar

- Você deve ter feito backup do recurso ou dos grupos de recursos.
- Você deve ter cancelado qualquer operação de backup que esteja em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos de pré-restauração, pós-restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-*

in Creator\etc\allowed_commands.config

- Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

Sobre esta tarefa

- Para recursos descobertos automaticamente, a restauração é suportada com SFSR.
- A recuperação automática em um momento específico e em minutos não é suportada.
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com o tipo, host, grupos de recursos e políticas associados e status.

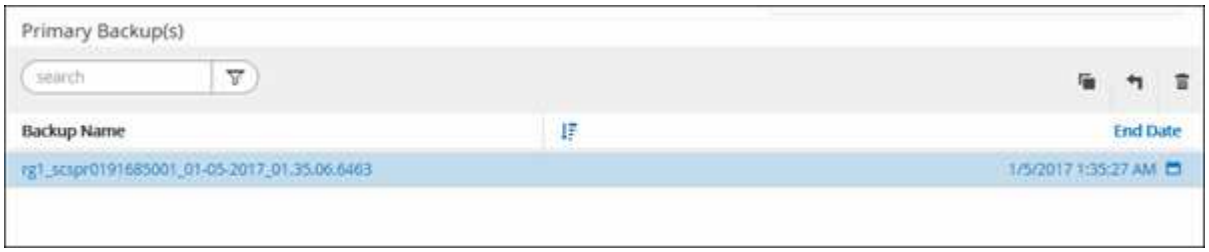
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, “Não protegido” será exibido na coluna Status geral. Isso pode significar que o recurso não está protegido ou que o backup do recurso foi feito por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e depois selecione um recurso nesse grupo.

   A página de topologia de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela Backup(s) primário(s), selecione o backup que deseja restaurar e clique em *  *.



6. Na página Escopo de restauração, selecione **Recurso completo** para restaurar os volumes de dados configurados do banco de dados MySQL.
7. Na página Pré-operações, insira os comandos pre restore e unmount para executar antes de realizar um trabalho de restauração.

   Os comandos de desmontagem não estão disponíveis para recursos descobertos automaticamente.

8. Na página Post ops, insira os comandos mount e post restore para serem executados após realizar um trabalho de restauração.

Os comandos de montagem não estão disponíveis para recursos descobertos automaticamente.

9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O SMTP também deve ser configurado na página **Configurações** > **Configurações globais**.

10. Revise o resumo e clique em **Concluir**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Restaurar recursos usando cmdlets do PowerShell

Restaurar um backup de recursos inclui iniciar uma sessão de conexão com o SnapCenter Server, listar os backups e recuperar informações de backup, além de restaurar um backup.

Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
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
```

   Este exemplo exibe informações detalhadas sobre o backup de 29 de janeiro de 2015 a 3 de fevereiro de 2015:

```
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. Restaure os dados do backup usando o cmdlet Restore-SmBackup.

```
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           :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitorar operações de restauração do MySQL

Você pode monitorar o progresso de diferentes operações de restauração do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa tomar.

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento

- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de restauração sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Restaurar**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Aplicar** para visualizar as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Clonar backups de recursos do MySQL

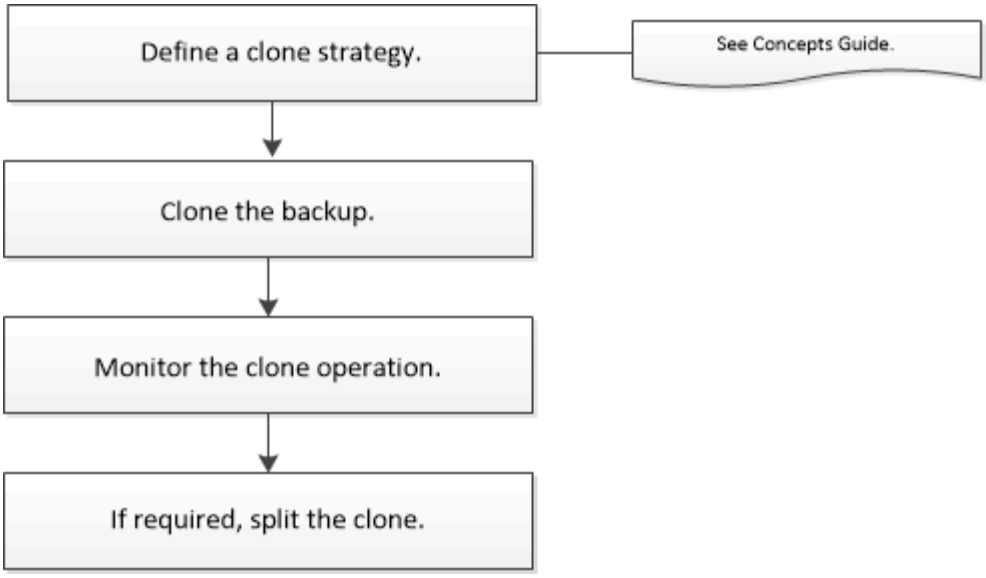
Fluxo de trabalho de clonagem

O fluxo de trabalho de clonagem inclui executar a operação de clonagem e monitorar a operação.

Sobre esta tarefa

- Você pode clonar no servidor MySQL de origem.
- Você pode clonar backups de recursos pelos seguintes motivos:
  - Para testar a funcionalidade que deve ser implementada usando a estrutura e o conteúdo atuais dos recursos durante os ciclos de desenvolvimento do aplicativo
  - Para ferramentas de extração e manipulação de dados ao preencher data warehouses
  - Para recuperar dados que foram excluídos ou alterados por engano

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de clonagem:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre os cmdlets do PowerShell.

Clonar um backup do MySQL

Você pode usar o SnapCenter para clonar um backup. Você pode clonar a partir do backup primário ou secundário.

Antes de começar

- Você deve ter feito backup dos recursos ou do grupo de recursos.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de armazenamento (SVM).
- Para comandos de pré-clonagem ou pós-clonagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in nos seguintes caminhos:
  - Local padrão no host do Windows: *C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Local padrão no host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

> Se os comandos não existirem na lista de comandos, a operação falhará. * Para a versão MySQL 5.7, você deve definir IGNORE_MYSQLX_PORT = true (por padrão, false) no arquivo de propriedades do MySQL.

Sobre esta tarefa

- Você não pode proteger as instâncias clonadas do MySQL.
- Para obter informações sobre as operações de divisão de volume do FlexClone , consultehttps://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html["Dividir um volume FlexClone de seu volume pai"] .
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos Snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com informações como tipo, host, grupos de recursos e políticas associados e status.

3. Selecione o recurso ou grupo de recursos.

   Você deve selecionar um recurso se selecionar um grupo de recursos.

   A página de topologia de recurso ou grupo de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Selecione o backup de dados da tabela e clique em  .
6. Na página Localização, execute as seguintes ações:

Para este campo…	Faça isso…
Servidor clone	Escolha um host no qual o clone deve ser criado.
Porta	Forneça a porta na qual a instância clonada do MySQL será iniciada.
Endereço IP de exportação NFS	Insira os endereços IP ou os nomes de host nos quais os volumes clonados serão exportados.

7. Na página Scripts, execute as seguintes etapas:

   Os scripts são executados no host do plug-in.

   a. Insira os comandos para pré-clonagem ou pós-clonagem que devem ser executados antes ou depois da operação de clonagem, respectivamente.
      - Comando pré-clone: exclui bancos de dados existentes com o mesmo nome
      - Comando post clone: verifica um banco de dados ou inicia um banco de dados.
   b. Digite o comando mount para montar um sistema de arquivos em um host.

      Comando de montagem para um volume ou qtree em uma máquina Linux:

   Exemplo para NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail.

9. Revise o resumo e clique em **Concluir**.
10. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

```
PS C:\> Open-SmConnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

2. Recupere os backups para executar a operação de clonagem usando o cmdlet Get-SmBackup.

   Este exemplo mostra que dois backups estão disponíveis para clonagem:

```
 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. Inicie uma operação de clonagem a partir de um backup existente e especifique os endereços IP de exportação do NFS nos quais os volumes clonados serão exportados.

   Este exemplo mostra que o backup a ser clonado tem um endereço NFSExportIPs de 10.32.212.14:

```
PS C:\> New-SmClone -AppPluginCode MySQL -BackupName
"scs000211748_gdl_englab_netapp_com_MySQL_mysqld_3306_scs000211748_0
6-26-2024_06.08.35.4307" -Resources
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306"}
-Port 3320 -CloneToHost shivarhel30.rtp.openenglab.netapp.com
```

   Se NFSExportIPs não for especificado, o padrão será exportado para o host de destino do clone.

4. Verifique se os backups foram clonados com sucesso usando o cmdlet Get-SmCloneReport para visualizar os detalhes do trabalho de clonagem.

   Você pode visualizar detalhes como ID do clone, data e hora de início, data e hora de término.

```
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          :
```

Monitorar operações de clonagem do MySQL

Você pode monitorar o progresso das operações de clonagem do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.

3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente operações de clonagem sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione o trabalho de clonagem e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página Detalhes do trabalho, clique em **Exibir registros**.

Dividir um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido se torna independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clone em um clone intermediário.

  Por exemplo, depois de criar o clone1 a partir de um backup de banco de dados, você pode criar um backup do clone1 e então clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e você não pode executar a operação de divisão de clone no clone1. No entanto, você pode executar a operação de divisão de clone no clone2.

  Após dividir o clone2, você pode executar a operação de divisão do clone no clone1 porque o clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e os trabalhos de clonagem do clone são excluídos.
- Para obter informações sobre as operações de divisão de volume do FlexClone , consulte "Dividir um volume FlexClone de seu volume pai" .
- Certifique-se de que o volume ou agregado no sistema de armazenamento esteja online.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página **Recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicações de banco de dados	Selecione **Banco de dados** na lista Exibir.
Para sistemas de arquivos	Selecione **Caminho** na lista Exibir.

3. Selecione o recurso apropriado na lista.

   A página de topologia de recursos é exibida.

4. Na exibição **Gerenciar cópias**, selecione o recurso clonado (por exemplo, o banco de dados ou LUN) e clique em * * .
5. Revise o tamanho estimado do clone que será dividido e o espaço necessário disponível no agregado e

clique em **Iniciar**.

6. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

   A operação de divisão do clone para de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clone e, em seguida, tentar novamente a operação de divisão de clone.

   Se você quiser um tempo de pesquisa maior ou menor para verificar se o clone está dividido ou não, você pode alterar o valor do parâmetro *CloneSplitStatusCheckPollTime* no arquivo *SMCoreServiceHost.exe.config* para definir o intervalo de tempo para o SMCore pesquisar o status da operação de divisão do clone. O valor está em milissegundos e o valor padrão é 5 minutos.

   Por exemplo:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   A operação de início da divisão do clone falha se um backup, uma restauração ou outra divisão do clone estiver em andamento. Você deve reiniciar a operação de divisão do clone somente após a conclusão das operações em execução.

Informações relacionadas

"O clone ou a verificação do SnapCenter falham com o agregado inexistente"

Excluir ou dividir clones de banco de dados MySQL após atualizar o SnapCenter

Após atualizar para o SnapCenter 4.3, você não verá mais os clones. Você pode excluir o clone ou dividir os clones na página Topologia do recurso a partir do qual os clones foram criados.

Sobre esta tarefa

Se você quiser localizar a pegada de armazenamento dos clones ocultos, execute o seguinte comando: `Get-SmClone -ListStorageFootprint`

Passos

1. Exclua os backups dos recursos clonados usando o cmdlet remove-smbackup.
2. Exclua o grupo de recursos dos recursos clonados usando o cmdlet remove-smresourcegroup.
3. Remova a proteção do recurso clonado usando o cmdlet remove-smprotectresource.
4. Selecione o recurso pai na página Recursos.

   A página de topologia de recursos é exibida.

5. Na exibição Gerenciar cópias, selecione os clones dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
6. Selecione os clones e clique em  para excluir clones ou clicar  para dividir os clones.
7. Clique em **OK**.

Proteja aplicativos usando plug-ins compatíveis com NetApp

Plug-ins suportados pela NetApp

Visão geral dos plug-ins suportados pela NetApp

Você pode usar os plug-ins suportados NetApp , como MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB e plug-in de armazenamento para os aplicativos que você usa e, em seguida, usar o SnapCenter para fazer backup, restaurar ou clonar esses aplicativos. Os plug-ins suportados NetApp atuam como componentes do lado do host do NetApp SnapCenter Software, permitindo a proteção de dados com reconhecimento de aplicativo e o gerenciamento de recursos.

Quando os plug-ins suportados NetApp estiverem instalados, você poderá usar o SnapCenter com a tecnologia NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e usar a tecnologia NetApp SnapVault para executar a replicação de backup de disco para disco. Os plug-ins suportados pela NetApp podem ser usados em ambientes Windows e Linux.

O SnapCenterCLI não oferece suporte a comandos de plug-ins suportados NetApp .

A NetApp fornece o plug-in de armazenamento para executar operações de proteção de dados do volume de dados no armazenamento ONTAP usando a estrutura de plug-in integrada ao SnapCenter.

Você pode instalar os plug-ins suportados pela NetApp na página Adicionar Host.

"Adicione hosts e instale pacotes de plug-ins em hosts remotos."

A política de suporte do SnapCenter cobrirá o suporte para a estrutura do plug-in, o mecanismo principal e as APIs associadas. O suporte não cobrirá o código-fonte do plug-in e os scripts associados criados na estrutura do plug-in.

O que você pode fazer com os plug-ins suportados pela NetApp

Você pode usar os plug-ins suportados pela NetApp , como MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB e plug-in de armazenamento para operações de proteção de dados.

- Adicione recursos como bancos de dados, instâncias, documentos ou tablespaces.
- Crie backups.
- Restaurar a partir de backups.
- Clonar backups.
- Agende operações de backup.
- Monitore operações de backup, restauração e clonagem.
- Visualize relatórios de operações de backup, restauração e clonagem.

Você pode usar os plug-ins suportados pela NetApp para operações de proteção de dados.

- Faça snapshots do grupo de consistência dos volumes de armazenamento em clusters ONTAP .
- Faça backup de aplicativos personalizados usando a estrutura de pré e pós-script integrada

  Você pode fazer backup de um volume ONTAP , LUN ou Qtree.

- Atualizar instantâneos tirados do primário para um secundário ONTAP , aproveitando o relacionamento de replicação existente (SnapVault/ SnapMirror/replicação unificada) usando a política do SnapCenter

  ONTAP primário e secundário podem ser ONTAP FAS, AFF, ASA, ONTAP Select ou Cloud Volumes ONTAP.

- Recupere volumes ONTAP , LUN ou arquivos completos.

  Você deve fornecer o caminho do arquivo respectivo manualmente, pois os recursos de navegação ou indexação não estão incorporados ao produto.

  A restauração de Qtree ou diretório não é suportada, mas você pode clonar e exportar somente o Qtree se o escopo de backup estiver definido no nível do Qtree.

Recursos de plug-ins suportados pela NetApp

O SnapCenter integra-se ao aplicativo plug-in e às tecnologias NetApp no sistema de armazenamento. Para trabalhar com plug-ins compatíveis com NetApp , como MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB e plug-in de armazenamento, use a interface gráfica do usuário do SnapCenter .

- **Interface gráfica de usuário unificada**

  A interface do SnapCenter fornece padronização e consistência entre plug-ins e ambientes. A interface do SnapCenter permite que você conclua operações consistentes de backup, restauração, recuperação e clonagem em plug-ins, use relatórios centralizados, use visualizações de painel rápidas, configure o controle de acesso baseado em função (RBAC) e monitore trabalhos em todos os plug-ins.

- **Administração central automatizada**

  Você pode agendar operações de backup, configurar retenção de backup baseada em políticas e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- **Tecnologia NetApp Snapshot não disruptiva**

  O SnapCenter usa a tecnologia NetApp Snapshot com os plug-ins suportados pela NetApp para fazer backup de recursos. Os instantâneos consomem espaço de armazenamento mínimo.

Os plug-ins suportados pela NetApp também oferecem os seguintes benefícios:

- Suporte para fluxos de trabalho de backup, restauração e clonagem
- Segurança com suporte RBAC e delegação centralizada de funções

  Você também pode definir as credenciais para que os usuários autorizados do SnapCenter tenham permissões no nível do aplicativo.

- Criação de cópias de recursos com eficiência de espaço e em um determinado momento para testes ou extração de dados usando a tecnologia NetApp FlexClone

  Uma licença FlexClone é necessária no sistema de armazenamento onde você deseja criar o clone.

- Suporte para o recurso Snapshot do grupo de consistência (CG) do ONTAP como parte da criação de backups.
- Capacidade de executar vários backups simultaneamente em vários hosts de recursos

  Em uma única operação, os Snapshots são consolidados quando recursos em um único host compartilham o mesmo volume.

- Capacidade de criar Snapshot usando comandos externos.
- Capacidade de criar instantâneos consistentes do sistema de arquivos em ambientes Windows.

Tipos de armazenamento suportados pelos plug-ins suportados pela NetApp

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e virtuais. Você deve verificar o suporte para seu tipo de armazenamento antes de instalar plug-ins compatíveis com o NetApp .

Máquina	Tipo de armazenamento
Montagens físicas e diretas NFS nos hosts de VM (VMDKs e RDM LUNs não são suportados).	LUNs conectados por FC
Montagens físicas e diretas NFS nos hosts de VM (VMDKs e RDM LUNs não são suportados).	LUNs conectados por iSCSI
Montagens físicas e diretas NFS nos hosts de VM (VMDKs e RDM LUNs não são suportados).	Volumes conectados ao NFS
VMware ESXi	Armazenamentos de dados vVol em NFS e SAN O armazenamento de dados vVol só pode ser provisionado com o ONTAP Tools para VMware vSphere.

Privilégios ONTAP mínimos necessários para plug-in compatível com NetApp

Os privilégios mínimos do ONTAP necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos de acesso total: privilégios mínimos necessários para ONTAP 9.12.1 e posterior
  - evento generate-autosupport-log
  - histórico de trabalho mostrar
  - parada de trabalho
  - mostrar atributo lun

- lun criar
- lun delete
- geometria lunar
- lun igroup adicionar
- lun igroup criar
- lun igroup excluir
- renomear lun igroup
- show do lun igroup
- mapeamento lun add-reporting-nodes
- criação de mapeamento lun
- exclusão de mapeamento lun
- mapeamento lun remove-reporting-nodes
- show de mapeamento lunar
- lun modificar
- volume de entrada lun
- lua offline
- lua online
- redimensionamento de lun
- série lun
- show de lua
- interface de rede
- política de adição de regra do snapmirror
- regra de modificação de política do snapmirror
- política de remoção do snapmirror
- política do snapmirror mostrar
- restauração do snapmirror
- show de espelhos instantâneos
- histórico de exibição do snapmirror
- atualização do snapmirror
- atualização do snapmirror-ls-set
- lista-destinos do snapmirror
- versão
- criação de clone de volume
- show de clones de volume
- volume clone split start
- volume clone divisão parada
- volume criar

    - destruição de volume
    - clone de arquivo de volume criar
    - arquivo de volume mostrar-uso-do-disco
    - volume offline
    - volume on-line
    - modificação de volume
    - volume qtree criar
    - volume qtree delete
    - volume qtree modificar
    - volume qtree mostrar
    - restrição de volume
    - show de volume
    - criação de instantâneo de volume
    - exclusão de instantâneo de volume
    - modificação de instantâneo de volume
    - renomeação de instantâneo de volume
    - restauração de instantâneo de volume
    - arquivo de restauração de instantâneo de volume
    - exibição de instantâneo de volume
    - desmontagem de volume
    - cifs do vserver
    - vserver cifs compartilhar criar
    - vserver cifs compartilhar excluir
    - vserver cifs shadowcopy mostrar
    - vserver cifs compartilhar mostrar
    - vserver cifs mostrar
    - criação de política de exportação do vserver
    - exclusão da política de exportação do vserver
    - criação de regra de política de exportação do vserver
    - mostrar regra de política de exportação do vserver
    - mostrar política de exportação do vserver
    - mostrar conexão iscsi do vserver
    - vserver mostrar
- Comandos somente leitura: privilégios mínimos necessários para ONTAP 8.3.0 e posterior
    - interface de rede

Preparar sistemas de armazenamento para replicação SnapMirror e SnapVault para plug-ins compatíveis com NetApp

Você pode usar um plug-in SnapCenter com a tecnologia ONTAP SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia ONTAP SnapVault para executar replicação de backup de disco para disco para conformidade com padrões e outros propósitos relacionados à governança. Antes de executar essas tarefas, você deve configurar um relacionamento de proteção de dados entre os volumes de origem e destino e inicializar o relacionamento.

O SnapCenter executa as atualizações no SnapMirror e no SnapVault após concluir a operação Snapshot. As atualizações do SnapMirror e do SnapVault são executadas como parte do trabalho do SnapCenter ; não crie uma programação ONTAP separada.

Se você estiver acessando o SnapCenter a partir de um produto NetApp SnapManager e estiver satisfeito com os relacionamentos de proteção de dados configurados, pode pular esta seção.

Um relacionamento de proteção de dados replica dados do armazenamento primário (o volume de origem) para o armazenamento secundário (o volume de destino). Quando você inicializa o relacionamento, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não oferece suporte a relacionamentos em cascata entre volumes SnapMirror e SnapVault (**Primário** > **Espelho** > **Cofre**). Você deve usar relacionamentos fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis em termos de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis em termos de versão e como configurá-los, consulte "Documentação do ONTAP" .

Definir uma estratégia de backup

Definir uma estratégia de backup antes de criar suas tarefas de backup garante que você tenha os backups necessários para restaurar ou clonar seus recursos com sucesso. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (RTO) e objetivo de ponto de recuperação (RPO) determinam em grande parte sua estratégia de backup.

Sobre esta tarefa

Um SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. RTO é o tempo em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. SLA, RTO e RPO contribuem para a estratégia de proteção de dados.

Passos

1. Determine quando você deve fazer backup dos seus recursos.
2. Decida quantos trabalhos de backup você precisa.
3. Decida como nomear seus backups.
4. Decida se você deseja Snapshots do Grupo de Consistência e decida sobre as opções apropriadas para excluir Snapshots do Grupo de Consistência.

5. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção de longo prazo.
6. Determine o período de retenção dos Snapshots no sistema de armazenamento de origem e no destino do SnapMirror .
7. Determine se você deseja executar algum comando antes ou depois da operação de backup e forneça uma prescrição ou pós-escrito.

Estratégia de backup para plug-ins suportados pela NetApp

Cronogramas de backup de recursos de plug-in suportados NetApp

O fator mais crítico na determinação de um cronograma de backup é a taxa de alteração do recurso. Quanto mais você fizer backup dos seus recursos, menos logs de arquivamento o SnapCenter terá que usar para restauração, o que pode resultar em operações de restauração mais rápidas.

Você pode fazer backup de um recurso muito utilizado a cada hora, enquanto pode fazer backup de um recurso raramente utilizado uma vez por dia. Outros fatores incluem a importância do recurso para sua organização, seu acordo de nível de serviço (SLA) e seu objetivo de ponto de recuperação (RPO).

O SLA define o nível de serviço esperado e aborda muitas questões relacionadas ao serviço, incluindo a disponibilidade e o desempenho do serviço. O RPO define a estratégia para a idade dos arquivos que devem ser recuperados do armazenamento de backup para que as operações regulares sejam retomadas após uma falha. SLA e RPO contribuem para a estratégia de proteção de dados.

Os agendamentos de backup têm duas partes, conforme a seguir:

- Frequência de backup

  A frequência de backup (com que frequência os backups devem ser realizados), também chamada de tipo de agendamento para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como horária, diária, semanal ou mensal. Você pode acessar políticas na GUI do SnapCenter clicando em **Configurações** > **Políticas**.

- Agendamentos de backup

  Os agendamentos de backup (exatamente quando os backups devem ser executados) fazem parte de uma configuração de recurso ou grupo de recursos. Por exemplo, se você tiver um grupo de recursos com uma política configurada para backups semanais, poderá configurar o agendamento para fazer backup toda quinta-feira às 22h. Você pode acessar os agendamentos do grupo de recursos na GUI do SnapCenter clicando em **Recursos**, selecionando o plug-in apropriado e clicando em **Exibir** > **Grupo de recursos**.

Número de trabalhos de backup necessários

Os fatores que determinam o número de tarefas de backup necessárias incluem o tamanho do recurso, o número de volumes usados, a taxa de alteração do recurso e seu Contrato de Nível de Serviço (SLA).

O número de tarefas de backup que você escolhe normalmente depende do número de volumes nos quais você colocou seus recursos. Por exemplo, se você colocar um grupo de recursos pequenos em um volume e um recurso grande em outro volume, você poderá criar uma tarefa de backup para os recursos pequenos e

uma tarefa de backup para o recurso grande.

Tipos de estratégias de restauração suportadas para recursos de plug-in suportados pela NetApp adicionados manualmente

Você deve definir uma estratégia antes de poder executar com sucesso operações de restauração usando o SnapCenter. Há dois tipos de estratégias de restauração para recursos de plug-in suportados NetApp adicionados manualmente.

Não é possível recuperar recursos de plug-in suportados NetApp adicionados manualmente.

Restauração completa de recursos

- Restaura todos os volumes, qtrees e LUNs de um recurso

Se o recurso contiver volumes ou qtrees, os Snapshots tirados após o Snapshot selecionado para restauração nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

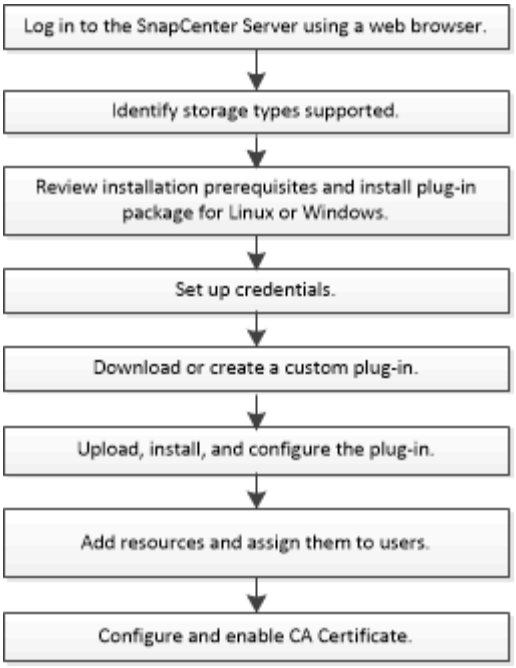
Restauração em nível de arquivo

- Restaura arquivos de volumes, qtrees ou diretórios
- Restaura apenas os LUNs selecionados

Prepare-se para instalar plug-ins compatíveis com NetApp

Fluxo de trabalho de instalação de plug-ins compatíveis com SnapCenter NetApp

Você deve instalar e configurar plug-ins compatíveis com o SnapCenter NetApp se quiser proteger os recursos de plug-ins compatíveis com o NetApp .



Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Windows, Linux ou AIX

Antes de adicionar um host e instalar os pacotes de plug-ins, você deve atender a todos os requisitos. Os plug-ins suportados pela NetApp são suportados em ambientes Windows, Linux e AIX.

Aplicativos de armazenamento e Oracle são suportados no AIX.

- Você deve ter instalado o Java 11 no seu host Linux, Windows ou AIX.

  O IBM Java não é suportado em hosts Windows e Linux.

- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.
- Os plug-ins suportados NetApp , como MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB e plug-in de armazenamento, devem estar disponíveis no host do cliente de onde a operação de adição de host é realizada.

Em geral

Se você estiver usando iSCSI, o serviço iSCSI deverá estar em execução.

Hosts do Windows

- Você deve ter um usuário de domínio com privilégios de administrador local e permissões de login local no host remoto.
- Se você gerenciar nós de cluster no SnapCenter, deverá ter um usuário com privilégios administrativos para todos os nós do cluster.

- Você deve escolher manualmente o SnapCenter Plug-in para Microsoft Windows.

  "Baixe JAVA para Windows"

Hosts Linux e AIX

Aplicativos de armazenamento e Oracle são suportados no AIX.

- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.
- Você deve ter instalado o Java 11 no seu host Linux.

  Se estiver usando o Windows Server 2019 ou o Windows Server 2016 para o host do SnapCenter Server, você deverá instalar o Java 11. A Ferramenta de Matriz de Interoperabilidade (IMT) contém as informações mais recentes sobre requisitos.

  "Baixe JAVA para Linux"

  "Baixe JAVA para AIX"

  "Ferramenta de Matriz de Interoperabilidade da NetApp"

- Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos. Adicione as seguintes linhas ao arquivo /etc/sudoers usando o utilitário visudo Linux.

  Certifique-se de estar usando o Sudo versão 1.8.7 ou posterior.

```
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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

  LINUX_USER é o nome do usuário não root que você criou.

Você pode obter o *checksum_value* do arquivo **sc_unix_plugins_checksum.txt**, localizado em:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Linux.

> O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Requisitos do host AIX

Você deve garantir que o host atenda aos requisitos antes de instalar o Pacote de plug-ins do SnapCenter para AIX.

> Aplicativos de armazenamento e Oracle são suportados no AIX.

> O SnapCenter Plug-in para UNIX, que faz parte do Pacote de Plug-ins SnapCenter para AIX, não oferece suporte a grupos de volumes simultâneos.

Item	Requisitos
Sistemas operacionais	AIX 7.1 ou posterior
RAM mínima para o plug-in SnapCenter no host	4 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	2 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	Java 11 IBM Java Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em /var/opt/snapcenter/spl/etc/spl.properties esteja definida para a versão correta do JAVA e o caminho correto.

Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Configurar privilégios sudo para usuários não root para host AIX

O SnapCenter 4.4 e versões posteriores permitem que um usuário não root instale o Pacote de plug-ins do SnapCenter para AIX e inicie o processo de plug-in. Os processos do plug-in serão executados como um usuário não root efetivo. Você deve configurar privilégios sudo para que o usuário não root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos do código de autenticação de mensagens: MACs hmac-sha2-256 e MACs hmac-sha2-512.

  Reinicie o serviço sshd após atualizar o arquivo de configuração.

  Exemplo:

```
#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
```

Sobre esta tarefa

Você deve configurar privilégios sudo para que o usuário não root forneça acesso aos seguintes caminhos:

- /home/*AIX_USER*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /localização_personalizada/ NetApp/snapcenter/spl/instalação/plugins/desinstalação
- /localização_personalizada/ NetApp/snapcenter/spl/bin/spl

Passos

1. Efetue login no host AIX no qual você deseja instalar o Pacote de plug-ins do SnapCenter para AIX.
2. Adicione as seguintes linhas ao arquivo /etc/sudoers usando o utilitário visudo Linux.

```
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
```

Se você tiver uma configuração RAC, junto com os outros comandos permitidos, você deve adicionar o seguinte ao arquivo /etc/sudoers: '/<crs_home>/bin/olsnodes'

Você pode obter o valor de *crs_home* do arquivo */etc/oracle/olr.loc*.

AIX_USER é o nome do usuário não root que você criou.

Você pode obter o *checksum_value* do arquivo **sc_unix_plugins_checksum.txt**, localizado em:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se o SnapCenter Server estiver instalado no host Linux.

O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Windows

Antes de instalar o pacote de plug-ins do SnapCenter para Windows, você deve estar familiarizado com alguns requisitos básicos de espaço e dimensionamento do sistema host.

Item	Requisitos
Sistemas Operacionais	Microsoft Windows Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	5 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• Pacote de hospedagem do ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes) • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK O Java 11 Oracle Java e OpenJDK são necessários apenas para SAP HANA, IBM Db2, PostgreSQL, MySQL, plug-ins compatíveis com NetApp e outros aplicativos personalizados que podem ser instalados no host Windows. Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" . Para obter informações específicas sobre solução de problemas do .NET, consulte "A atualização ou instalação do SnapCenter falha em sistemas legados que não têm conectividade com a Internet."

Requisitos de host para instalar o pacote de plug-ins SnapCenter para Linux e AIX

Você deve garantir que o host atenda aos requisitos antes de instalar o Pacote de plug-ins do SnapCenter para Linux ou AIX.

Aplicativos de armazenamento e Oracle são suportados no AIX.

Item	Requisitos
Sistemas operacionais	• Red Hat Enterprise Linux • Oracle Linux • Servidor SUSE Linux Enterprise (SLES)
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	2 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	Java 11 Oracle Java ou OpenJDK Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em /var/opt/snapcenter/spl/etc/spl.properties esteja definida para a versão correta do JAVA e o caminho correto.

Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp"

Configurar credenciais para plug-ins compatíveis com NetApp

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter . Você deve criar credenciais para instalar plug-ins do SnapCenter e credenciais adicionais para executar operações de proteção de dados em bancos de dados ou sistemas de arquivos do Windows.

Antes de começar

- Hosts Linux ou AIX

  Você deve configurar credenciais para instalar plug-ins em hosts Linux ou AIX.

  Você deve configurar as credenciais para o usuário root ou para um usuário não root que tenha privilégios

sudo para instalar e iniciar o processo do plug-in.

Melhores práticas: embora você tenha permissão para criar credenciais para o Linux após implantar hosts e instalar plug-ins, a melhor prática é criar credenciais depois de adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

  Você deve configurar as credenciais do Windows antes de instalar plug-ins.

  Você deve configurar as credenciais com privilégios de administrador, incluindo direitos de administrador no host remoto.

- Aplicativos de plug-ins suportados pela NetApp

  O plug-in usa as credenciais selecionadas ou criadas ao adicionar um recurso. Se um recurso não exigir credenciais durante operações de proteção de dados, você poderá definir as credenciais como **Nenhum**.

Sobre esta tarefa

Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver privilégios de administrador completos, será necessário atribuir pelo menos os privilégios de grupo de recursos e backup ao nome de usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.
4. Na página **Credencial**, especifique as informações necessárias para configurar as credenciais:

Para este campo…	Faça isso…
Nome da credencial	Digite um nome para as credenciais.

Para este campo…	Faça isso…
Nome de usuário	Digite o nome de usuário e a senha que serão usados para autenticação. • Administrador de domínio ou qualquer membro do grupo de administradores Especifique o administrador do domínio ou qualquer membro do grupo de administradores no sistema em que você está instalando o plug-in SnapCenter . Os formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS\Nome do Usuário* ◦ *FQDN do domínio\Nome do usuário* • Administrador local (somente para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local integrado no sistema em que você está instalando o plug-in SnapCenter . Você pode especificar uma conta de usuário local que pertença ao grupo de administradores locais se a conta de usuário tiver privilégios elevados ou se o recurso de Controle de Acesso do Usuário estiver desabilitado no sistema host. O formato válido para o campo Nome de usuário é: *UserName*
Senha	Digite a senha usada para autenticação.
Tipo de autenticação	Selecione o tipo de autenticação que você deseja usar.
Use privilégios sudo	Marque a caixa de seleção **Usar privilégios sudo** se estiver criando credenciais para um usuário não root. Aplicável somente a usuários de Linux e AIX.

5. Clique em **OK**.

Depois de concluir a configuração das credenciais, talvez você queira atribuir a manutenção de credenciais a um usuário ou grupo de usuários na página Usuário e Acesso.

Configurar o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite que você crie uma Conta de Serviço Gerenciada de grupo (gMSA) que fornece gerenciamento automatizado de senhas de contas de serviço a partir de uma conta de domínio gerenciada.

Antes de começar

- Você deve ter um controlador de domínio do Windows Server 2016 ou posterior.
- Você deve ter um host Windows Server 2016 ou posterior, que seja membro do domínio.

Passos

1. Crie uma chave raiz do KDS para gerar senhas exclusivas para cada objeto no seu gMSA.
2. Para cada domínio, execute o seguinte comando no controlador de domínio do Windows: Add-KDSRootKey -EffectiveImmediately
3. Crie e configure seu gMSA:
   a. Crie uma conta de grupo de usuários no seguinte formato:

```
 domainName\accountName$
.. Adicione objetos de computador ao grupo.
.. Use o grupo de usuários que você acabou de criar para criar o
gMSA.
```

   Por exemplo,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correr `Get-ADServiceAccount` comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Habilite o módulo do Active Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando no PowerShell:

```
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. Reinicie seu host.

b. Instale o gMSA no seu host executando o seguinte comando no prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua privilégios administrativos ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no SnapCenter Server.

   O SnapCenter Server instalará os plug-ins selecionados no host e o gMSA especificado será usado como a conta de logon de serviço durante a instalação do plug-in.

Instalar os plug-ins suportados pela NetApp

Adicionar hosts e instalar pacotes de plug-ins em hosts remotos

Você deve usar a página Adicionar Host do SnapCenter para adicionar hosts e, em seguida, instalar os pacotes de plug-in. Os plug-ins são instalados automaticamente nos hosts remotos. Você pode adicionar um host e instalar os pacotes de plug-in para um host individual ou para um cluster.

Antes de começar

- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.
- Se estiver usando uma conta de serviço gerenciada em grupo (gMSA), você deverá configurar a gMSA com privilégios administrativos.

  "Configurar conta de serviço gerenciada de grupo no Windows Server 2016 ou posterior para aplicativos personalizados"

- Para o host Windows, você deve garantir que selecionou o SnapCenter Plug-in para Windows.

Sobre esta tarefa

- Não é possível adicionar um SnapCenter Server como um host de plug-in a outro SnapCenter Server.
- Se você instalar plug-ins em um cluster (WSFC), os plug-ins serão instalados em todos os nós do cluster.

Passos

1. No painel de navegação esquerdo, selecione **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Selecione **Adicionar**.
4. Na página Hosts, execute as seguintes ações:

Para este campo…	Faça isso…
Tipo de host	Selecione o tipo de host: • Windows • Linux • AIX Os plug-ins suportados pela NetApp podem ser usados em ambientes Windows, Linux e AIX. Aplicativos de armazenamento e Oracle são suportados no AIX.
Nome do host	Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o FQDN. Para ambientes Windows, o endereço IP é suportado para hosts de domínio não confiáveis somente se for resolvido para o FQDN. Você pode inserir os endereços IP ou FQDN de um host autônomo. Se você estiver adicionando um host usando o SnapCenter e o host fizer parte de um subdomínio, você deverá fornecer o FQDN.

Para este campo…	Faça isso…
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. As credenciais devem ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais. Você pode visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou. O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar Host.

5. Na seção **Selecionar plug-ins para instalar**, selecione os plug-ins a serem instalados.

   Você pode instalar os seguintes plug-ins da lista:

   - MongoDB
   - ORASCPM (exibido como Aplicativos Oracle)
   - SAP ASE
   - SAP MaxDB
   - Armazenar

6. (Opcional) Selecione **Mais opções** para instalar os outros plug-ins.

Para este campo…	Faça isso…
Porta	Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.

Para este campo…	Faça isso…
Caminho de instalação	Os plug-ins suportados pela NetApp podem ser instalados em um sistema Windows ou Linux. • Para o pacote de plug-ins SnapCenter para Windows, o caminho padrão é C:\Arquivos de Programas\ NetApp\ SnapCenter. Opcionalmente, você pode personalizar o caminho. • Para o pacote de plug-ins SnapCenter para Linux e o pacote de plug-ins SnapCenter para AIX, o caminho padrão é `/opt/NetApp/snapcenter` . Opcionalmente, você pode personalizar o caminho.
Ignorar verificações de pré-instalação	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.
Use a conta de serviço gerenciada em grupo (gMSA) para executar os serviços do plug-in	Para o host Windows, marque esta caixa de seleção se desejar usar a Conta de Serviço Gerenciada em Grupo (gMSA) para executar os serviços do plug-in. Forneça o nome do gMSA no seguinte formato: domainName\accountName$. O gMSA será usado como uma conta de serviço de logon somente para o serviço SnapCenter Plug-in para Windows.

7. Selecione **Enviar**.

Se você não tiver marcado a caixa de seleção **Ignorar pré-verificações**, o host será validado para verificar se atende aos requisitos para a instalação do plug-in. O espaço em disco, a RAM, a versão do PowerShell, a versão do .NET, a localização (para plug-ins do Windows) e a versão do Java (para plug-ins do Linux) são validados em relação aos requisitos mínimos. Se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas serão exibidas.

Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em `C:\Program Files\NetApp\SnapCenter WebApp` para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.

Em uma configuração de HA, se você estiver atualizando o SnapManager.Web.UI.dll.config, deverá atualizar o arquivo em ambos os nós e reiniciar o SnapCenter App Pool.

O caminho padrão do Windows é `C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config`

O caminho padrão do Linux é `/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config`

8. Se o tipo de host for Linux, verifique a impressão digital e selecione **Confirmar e Enviar**.

A verificação de impressão digital é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitore o progresso da instalação.

Os arquivos de log específicos da instalação estão localizados em `/custom_location/snapcenter/` registros.

Instalar pacotes de plug-in SnapCenter para Linux, Windows ou AIX em vários hosts remotos usando cmdlets

Você pode instalar os pacotes de plug-in do SnapCenter para Linux, Windows ou AIX em vários hosts simultaneamente usando o cmdlet Install-SmHostPackage do PowerShell.

Antes de começar

O usuário que adiciona um host deve ter direitos administrativos no host.

Aplicativos de armazenamento e Oracle são suportados no AIX.

Passos

1. Inicie o PowerShell.
2. No host do SnapCenter Server, estabeleça uma sessão usando o cmdlet Open-SmConnection e insira suas credenciais.
3. Instale o plug-in em vários hosts usando o cmdlet Install-SmHostPackage e os parâmetros necessários.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Você pode usar a opção -skipprecheck quando tiver instalado os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

4. Insira suas credenciais para instalação remota.

Instale os plug-ins suportados pela NetApp em hosts Linux usando a interface de linha de comando

Você deve instalar os plug-ins suportados NetApp usando a interface de usuário (IU) do SnapCenter . Se o seu ambiente não permitir a instalação remota do plug-in pela interface do usuário do SnapCenter , você poderá instalar os plug-ins suportados NetApp

no modo de console ou no modo silencioso usando a interface de linha de comando (CLI).

Passos

1. Copie o arquivo de instalação do pacote de plug-ins do SnapCenter para Linux (snapcenter_linux_host_plugin.bin) de C:\ProgramData\ NetApp\ SnapCenter\Package Repository para o host onde você deseja instalar os plug-ins suportados NetApp .

   Você pode acessar esse caminho a partir do host onde o SnapCenter Server está instalado.

2. No prompt de comando, navegue até o diretório onde você copiou o arquivo de instalação.
3. Instale o plug-in: `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 especifica a porta de comunicação HTTPS do SMCore.
   - -DSERVER_IP especifica o endereço IP do SnapCenter Server.
   - -DSERVER_HTTPS_PORT especifica a porta HTTPS do SnapCenter Server.
   - -DUSER_INSTALL_DIR especifica o diretório onde você deseja instalar o pacote de plug-ins do SnapCenter para Linux.
   - _DINSTALL_LOG_NAME especifica o nome do arquivo de log.

   ```
   /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. Adicione o host ao SnapCenter Server usando o cmdlet Add-Smhost e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

5. Efetue login no SnapCenter e carregue o plug-in compatível com NetApp a partir da interface do usuário ou usando cmdlets do PowerShell.

   Você pode carregar o plug-in compatível com NetApp a partir da IU consultando"Adicionar hosts e instalar pacotes de plug-ins em hosts remotos" seção.

   A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell.

   "Guia de referência do cmdlet do software SnapCenter" .

Monitore o status da instalação de plug-ins compatíveis com a NetApp

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar

quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
   a. Clique em **Filtrar**.
   b. Opcional: especifique a data de início e término.
   c. No menu suspenso Tipo, selecione **Instalação de plug-in**.
   d. No menu suspenso Status, selecione o status da instalação.
   e. Clique em **Aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Configurar certificado CA

Gerar arquivo CSR de certificado CA

Você pode gerar uma Solicitação de Assinatura de Certificado (CSR) e importar o certificado que pode ser obtido de uma Autoridade de Certificação (CA) usando o CSR gerado. O certificado terá uma chave privada associada a ele.

CSR é um bloco de texto codificado que é fornecido a um fornecedor de certificado autorizado para obter o certificado de CA assinado.

O comprimento mínimo da chave RSA do certificado CA deve ser de 3072 bits.

Para obter informações sobre como gerar um CSR, consulte "Como gerar um arquivo CSR de certificado CA" .

Se você possui o certificado CA para seu domínio (*.domain.company.com) ou seu sistema (machine1.domain.company.com), você pode pular a geração do arquivo CSR do certificado CA. Você pode implantar o certificado CA existente com o SnapCenter.

Para configurações de cluster, o nome do cluster (FQDN do cluster virtual) e os respectivos nomes de host

devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome Alternativo do Assunto (SAN) antes de adquirir o certificado. Para um certificado curinga (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados de CA

Você deve importar os certificados de CA para o SnapCenter Server e os plug-ins do host do Windows usando o console de gerenciamento da Microsoft (MMC).

Passos

1. Acesse o console de gerenciamento da Microsoft (MMC) e clique em **Arquivo** > **Adicionar/Remover Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **Certificados** e clique em **Adicionar**.
3. Na janela do snap-in Certificados, selecione a opção **Conta de computador** e clique em **Concluir**.
4. Clique em **Console Root** > **Certificados – Computador local** > **Autoridades de certificação raiz confiáveis** > **Certificados**.
5. Clique com o botão direito do mouse na pasta “Autoridades de Certificação Raiz Confiáveis” e selecione **Todas as Tarefas** > **Importar** para iniciar o assistente de importação.
6. Conclua o assistente da seguinte forma:

Nesta janela do assistente…	Faça o seguinte…
Importar chave privada	Selecione a opção **Sim**, importe a chave privada e clique em **Avançar**.
Formato de arquivo de importação	Não faça alterações; clique em **Avançar**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluindo o Assistente de Importação de Certificados	Revise o resumo e clique em **Concluir** para iniciar a importação.

> O certificado de importação deve ser agrupado com a chave privada (os formatos suportados são: *.pfx, *.p12 e *.p7b).

7. Repita a Etapa 5 para a pasta “Pessoal”.

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma sequência hexadecimal que identifica um certificado. Uma impressão digital é calculada a partir do conteúdo do certificado usando um algoritmo de impressão digital.

Passos

1. Execute o seguinte na GUI:
   a. Clique duas vezes no certificado.

b. Na caixa de diálogo Certificado, clique na guia **Detalhes**.

c. Percorra a lista de campos e clique em **Impressão digital**.

d. Copie os caracteres hexadecimais da caixa.

e. Remova os espaços entre os números hexadecimais.

Por exemplo, se a impressão digital for: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", após remover os espaços, será: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Execute o seguinte no PowerShell:

a. Execute o seguinte comando para listar a impressão digital do certificado instalado e identificar o certificado instalado recentemente pelo nome do assunto.

Get-ChildItem -Path Cert:\LocalMachine\My

b. Copie a impressão digital.

Configurar certificado CA com serviços de plug-in de host do Windows

Você deve configurar o certificado CA com os serviços de plug-in do host do Windows para ativar o certificado digital instalado.

Execute as seguintes etapas no SnapCenter Server e em todos os hosts de plug-in onde os certificados CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão 8145 do SMCore, executando o seguinte comando:

```
> netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
```

Por exemplo:

```
 > netsh http delete sslcert ipport=0.0.0.0:8145
. Vincule o certificado recém-instalado aos serviços de plug-in do host
do Windows, executando os seguintes comandos:
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Por exemplo:

```
> $cert = “a909502dd82ae41433e6f83886b00d4277a32a7b”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Configurar o certificado CA para o serviço de plug-ins suportados pela NetApp no host Linux

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo 'keystore.jks', que está localizado em */opt/ NetApp/snapcenter/scc/etc* como seu armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in a partir do arquivo de propriedades do agente do plug-in.

   É o valor correspondente à chave 'KEYSTORE_PASS'.

2. Alterar a senha do keystore:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Altere a senha de todos os aliases de entradas de chave privada no
   keystore para a mesma senha usada para o keystore:
   ```

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

3. Reinicie o serviço após alterar a senha.

   A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.

3. Listar os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione um certificado raiz ou intermediário:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Reinicie o serviço após configurar os certificados raiz ou
intermediários para conectar o trust-store.
```

Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Adicione o certificado da CA com chave privada e pública.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Listar os certificados adicionados no keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

   A senha padrão do keystore do plug-in é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

```
 keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Se o nome do alias no certificado da CA for longo e contiver espaços
ou caracteres especiais ("*",","), altere o nome do alias para um nome
simples:
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configure o nome do alias do certificado CA no arquivo
agent.properties.
```

Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

Configurar lista de revogação de certificados (CRL) para plug-ins

Sobre esta tarefa

- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é ' opt/NetApp/snapcenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties em relação à chave CRL_PATH.

   Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Configurar o certificado CA para o serviço de plug-ins suportados pela NetApp no host Windows

Você deve gerenciar a senha do keystore do plug-in e seu certificado, configurar o certificado da CA, configurar certificados raiz ou intermediários para o trust-store do plug-in e configurar o par de chaves assinadas pela CA para o trust-store do plug-in com o serviço de plug-ins do SnapCenter para ativar o certificado digital instalado.

Os plug-ins usam o arquivo *keystore.jks*, que está localizado em *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* como seu armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore de plug-in e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore do plug-in a partir do arquivo de propriedades do agente do plug-in.

   É o valor correspondente à chave *KEYSTORE_PASS*.

2. Alterar a senha do keystore:

   keytool -storepasswd -keystore keystore.jks

   > Se o comando "keytool" não for reconhecido no prompt de comando do Windows, substitua o comando keytool pelo seu caminho completo.

   C:\Arquivos de Programas\Java\<versão_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks

3. Altere a senha de todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:

   keytool -keypasswd -alias "nome_do_alias_no_certificado" -keystore keystore.jks

   Atualize o mesmo para a chave KEYSTORE_PASS no arquivo *agent.properties*.

4. Reinicie o serviço após alterar a senha.

   A senha para o keystore do plug-in e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para plug-in trust-store

Você deve configurar os certificados raiz ou intermediários sem a chave privada para conectar o trust-store.

Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

   keytool -list -v -keystore keystore.jks

4. Adicione um certificado raiz ou intermediário:

   keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks

5. Reinicie o serviço após configurar os certificados raiz ou intermediários para conectar o trust-store.

Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para plug-in trust-store

Você deve configurar o par de chaves assinadas pela CA para o trust-store do plug-in.

Passos

1. Navegue até a pasta que contém o keystore do plug-in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Localize o arquivo *keystore.jks*.
3. Listar os certificados adicionados no keystore:

   keytool -list -v -keystore keystore.jks

4. Adicione o certificado da CA com chave privada e pública.

   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS

5. Listar os certificados adicionados no keystore.

   keytool -list -v -keystore keystore.jks

6. Verifique se o keystore contém o alias correspondente ao novo certificado CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado CA para a senha do keystore.

   A senha padrão do keystore do plug-in é o valor da chave KEYSTORE_PASS no arquivo agent.properties.

   keytool -keypasswd -alias "nome_do_alias_no_certificado_da_CA" -keystore keystore.jks

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

   Atualize este valor em relação à chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para plug-in trust-store.

Configurar lista de revogação de certificados (CRL) para plug-ins SnapCenter

Sobre esta tarefa

- Para baixar o arquivo CRL mais recente para o certificado CA relacionado, consulte "Como atualizar o arquivo de lista de revogação de certificados no SnapCenter CA Certificate" .
- Os plug-ins do SnapCenter procurarão os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL dos plug-ins do SnapCenter é *'C:\Arquivos de Programas\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo *agent.properties* em relação à chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

   Os certificados recebidos serão verificados em relação a cada CRL.

Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *Get-SmCertificateSettings*.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.

5. Selecione **Ativar validação de certificado**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- * * indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- * * indica que o certificado CA foi validado com sucesso.
- * * indica que o certificado CA não pôde ser validado.
- * * indica que as informações de conexão não puderam ser recuperadas.

> Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Prepare-se para a proteção de dados

Pré-requisitos para usar os plug-ins suportados pela NetApp

Antes de usar os plug-ins suportados SnapCenter NetApp , o administrador do SnapCenter deve instalar e configurar o SnapCenter Server e executar as tarefas de pré-requisito.

- Instalar e configurar o SnapCenter Server.
- Efetue login no SnapCenter Server.
- Configure o ambiente SnapCenter adicionando conexões do sistema de armazenamento e criando credenciais, se aplicável.
- Adicione hosts, instale e carregue os plug-ins.
- Se aplicável, instale o Java 11 no host do plug-in.
- Se você tiver vários caminhos de dados (LIFs) ou uma configuração dNFS, poderá executar o seguinte usando a CLI do SnapCenter no host do banco de dados:
  - Por padrão, todos os endereços IP do host do banco de dados são adicionados à política de exportação de armazenamento NFS na máquina virtual de armazenamento (SVM) para os volumes clonados. Se você quiser ter um endereço IP específico ou restringir a um subconjunto de endereços IP, execute a CLI Set-PreferredHostIPsInStorageExportPolicy.
  - Se você tiver vários caminhos de dados (LIFs) em SVMs, o SnapCenter escolherá o caminho de dados (LIF) apropriado para montar o volume clonado NFS. No entanto, se você quiser especificar um caminho de dados específico (LIF), deverá executar a CLI Set-SvmPreferredDataPath. As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência de comandos do software SnapCenter" .
- Configure o SnapMirror e o SnapVault se desejar replicação de backup.
- Certifique-se de que a porta 9090 não esteja sendo usada por nenhum outro aplicativo no host.

  A porta 9090 deve ser reservada para uso por plug-ins suportados NetApp , além das outras portas exigidas pelo SnapCenter.

Como recursos, grupos de recursos e políticas são usados para proteger recursos de plug-in com suporte da NetApp

Antes de usar o SnapCenter, é útil entender os conceitos básicos relacionados às operações de backup, clonagem e restauração que você deseja executar. Você interage com recursos, grupos de recursos e políticas para diferentes operações.

- Os recursos geralmente são bancos de dados, sistemas de arquivos do Windows ou VMs que você faz backup ou clona com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host ou cluster.

  Ao executar uma operação em um grupo de recursos, você executa essa operação nos recursos definidos no grupo de recursos de acordo com o cronograma especificado para o grupo de recursos.

  Você pode fazer backup sob demanda de um único recurso ou de um grupo de recursos. Você também pode executar backups agendados para recursos individuais e grupos de recursos.

- As políticas especificam a frequência de backup, retenção de cópias, replicação, scripts e outras características das operações de proteção de dados.

  Ao criar um grupo de recursos, você seleciona uma ou mais políticas para esse grupo. Você também pode selecionar uma política ao executar um backup sob demanda para um único recurso.

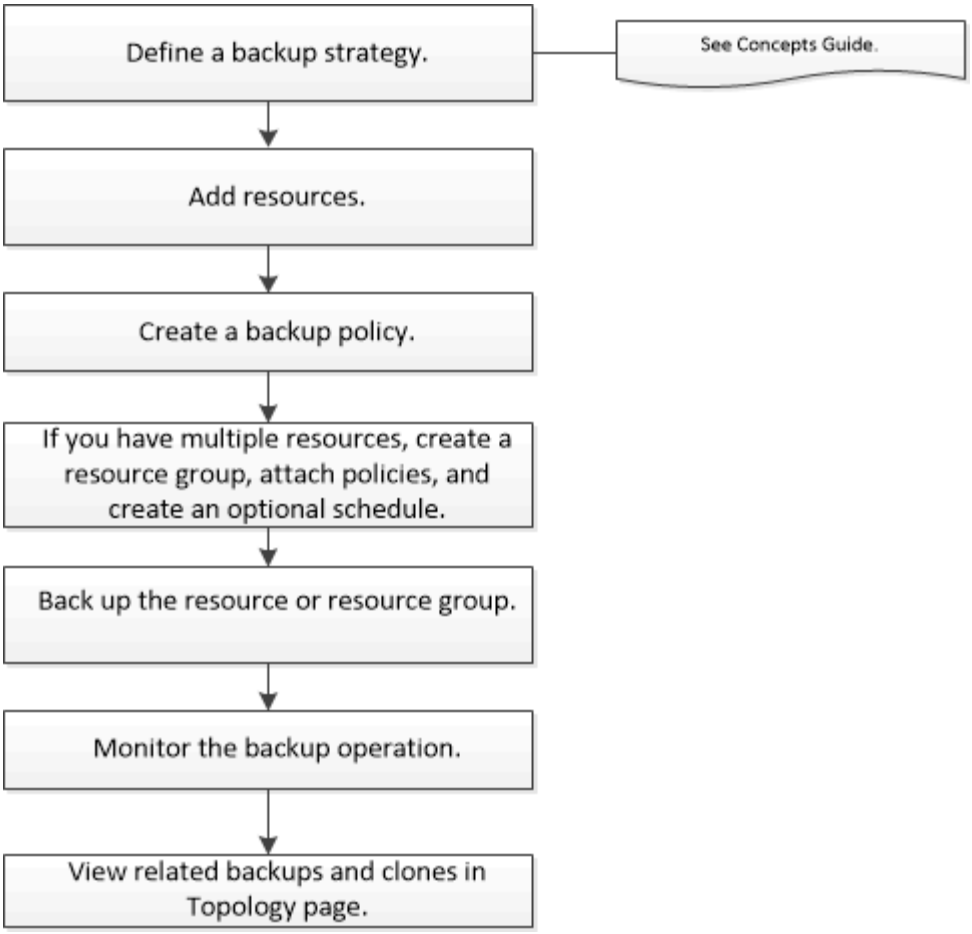
Pense em um grupo de recursos como definidor de *o que* você quer proteger e quando quer proteger em termos de dia e hora. Pense em uma política como a definição de *como* você quer protegê-la. Se você estiver fazendo backup de todos os bancos de dados ou de todos os sistemas de arquivos de um host, por exemplo, poderá criar um grupo de recursos que inclua todos os bancos de dados ou todos os sistemas de arquivos no host. Você pode então anexar duas políticas ao grupo de recursos: uma política diária e uma política horária. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup baseado em arquivo diariamente e outra programação que executa um backup baseado em instantâneo a cada hora.

Faça backup dos recursos de plug-ins suportados pela NetApp

Faça backup dos recursos de plug-ins suportados pela NetApp

O fluxo de trabalho de backup inclui planejamento, identificação de recursos para backup, gerenciamento de políticas de backup, criação de grupos de recursos e anexação de políticas, criação de backups e monitoramento das operações.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de backup:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet do SnapCenter ou consulte o "Guia de referência do cmdlet do software SnapCenter"

Adicionar recursos aos plug-ins suportados pela NetApp

Você deve adicionar os recursos que deseja fazer backup ou clonar. Dependendo do seu ambiente, os recursos podem ser instâncias de banco de dados ou coleções que você deseja fazer backup ou clonar.

Antes de começar

- Você deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts, criar conexões do sistema de armazenamento e adicionar credenciais.
- Você deve ter carregado os plug-ins no SnapCenter Server.

Passos

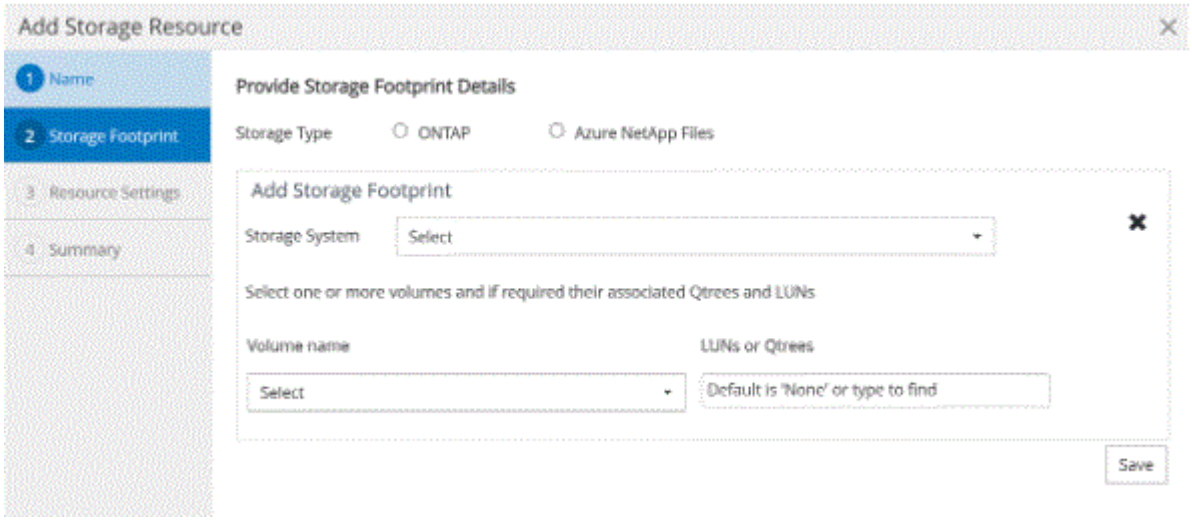
1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Adicionar Recurso**.
3. Na página Fornecer detalhes do recurso, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Digite o nome do recurso.
Nome do host	Selecione o host.
Tipo	Selecione o tipo. O tipo é definido pelo usuário conforme o arquivo de descrição do plug-in. Por exemplo, banco de dados e instância. Caso o tipo selecionado tenha um pai, insira os detalhes do pai. Por exemplo, se o tipo for Banco de Dados e o pai for Instância, insira os detalhes da Instância.
Nome da credencial	Selecione Credencial ou crie uma nova credencial.
Caminhos do Monte	Insira os caminhos de montagem onde o recurso está montado. Isso é aplicável somente para um host Windows.

4. Na página Fornecer espaço de armazenamento, selecione um sistema de armazenamento e escolha um ou mais volumes, LUNs e qtrees e, em seguida, selecione **Salvar**.

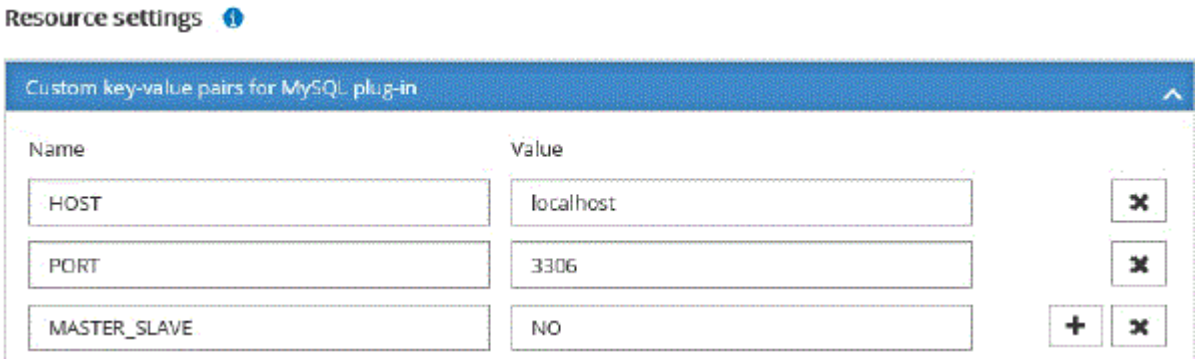
   Opcional: Selecione o + ícone para adicionar mais volumes, LUNs e qtrees de outros sistemas de armazenamento.

   Os plug-ins suportados pela NetApp não oferecem suporte à descoberta automática de recursos. Os detalhes de armazenamento de ambientes físicos e virtuais também não são descobertos automaticamente. Você deve fornecer as informações de armazenamento para ambientes físicos e virtuais ao criar os recursos.



5. Na página Configurações de recursos, forneça pares de chave-valor personalizados para o recurso.

Certifique-se de que o nome das chaves personalizadas esteja em letras maiúsculas.



Para os respectivos parâmetros do plug-in, consulte"Parâmetros para configurar o recurso"

6. Revise o resumo e selecione **Concluir**.

Resultado

Os recursos são exibidos junto com informações como tipo, nome do host ou cluster, grupos de recursos e políticas associados e status geral.

Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

Depois que você terminar

Se você quiser fornecer acesso aos ativos a outros usuários, o administrador do SnapCenter deverá atribuir ativos a esses usuários. Isso permite que os usuários executem as ações para as quais têm permissão nos ativos atribuídos a eles.

Depois de adicionar os recursos, você pode modificar os detalhes dos recursos. Se um recurso de plug-ins suportado NetApp tiver backups associados a ele, os seguintes campos não poderão ser modificados: nome do recurso, tipo de recurso e nome do host.

Parâmetros para configurar o recurso

Se estiver adicionando os plug-ins manualmente, você poderá usar os seguintes parâmetros para configurar o recurso na página Configurações do recurso.

Plug-in para MongoDB

Configurações de recursos:

- MONGODB_APP_SERVER=(para tipo de recurso como cluster fragmentado) ou MONGODB_REPLICASET_SERVER=(para tipo de recurso como replicaset)
- OPLOG_PATH=(Parâmetro opcional caso seja fornecido pelo MongoDB.propertiesfile)
- MONGODB_AUTHENTICATION_TYPE= (PLAIN para autenticação LDAP e None para outros)

Você deve fornecer os seguintes parâmetros que precisam ser fornecidos no arquivo MongoDB.properties:

- DESATIVAR_INICIAR_PARAR_SERVIÇOS=
  - N se os serviços de início/parada forem executados pelo plug-in.
  - Y se os serviços de início/parada forem executados pelo usuário.

    - O parâmetro opcional como valor padrão é definido como N.
- OPLOG_PATH_= (Parâmetro opcional caso já seja fornecido como par chave-valor personalizado no SnapCenter).

Plug-in para MaxDB

Configurações de recursos:

- XUSER_ENABLE (S|N) habilita ou desabilita o uso de um xuser para MaxDB para que uma senha não seja necessária para o usuário do banco de dados.
- HANDLE_LOGWRITER (S|N) executa operações de suspensão do logwriter (N) ou retomada do logwriter (S).
- DBMCLICMD (path_to_dbmcli_cmd) especifica o caminho para o comando MaxDB dbmcli. Se não for definido, dbmcli será usado no caminho de pesquisa.

Para o ambiente Windows, o caminho deve estar entre aspas duplas ("…").

- SQLCLICMD (path_to_sqlcli_cmd) especifica o caminho para o comando sqlcli do MaxDB. Se o caminho não estiver definido, sqlcli será usado no caminho de pesquisa.
- MAXDB_UPDATE_HIST_LOG (S|N) instrui o programa de backup do MaxDB sobre se ele deve atualizar o log de histórico do MaxDB.
- MAXDB_CHECK_SNAPSHOT_DIR: Exemplo, SID1:directory[,directory…]; [SID2:directoary[,directory…] verifica se uma operação de cópia do Snap Creator Snapshot foi bem-sucedida e garante que o snapshot seja criado.

  Isso se aplica somente ao NFS. O diretório deve apontar para o local que contém o diretório .snapshot. Vários diretórios podem ser incluídos em uma lista separada por vírgulas.

  No MaxDB 7.8 e versões posteriores, a solicitação de backup do banco de dados é marcada como Falha no histórico de backup.

- MAXDB_BACKUP_TEMPLATES: Especifica um modelo de backup para cada banco de dados.

  O modelo deve existir e ser um tipo externo de modelo de backup. Para habilitar a integração de snapshots para o MaxDB 7.8 e versões posteriores, você deve ter a funcionalidade do servidor em segundo plano do MaxDB e o modelo de backup do MaxDB já configurado do tipo EXTERNAL.

- MAXDB_BG_SERVER_PREFIX: Especifica o prefixo para o nome do servidor em segundo plano.

  Se o parâmetro MAXDB_BACKUP_TEMPLATES estiver definido, você também deverá definir o parâmetro MAXDB_BG_SERVER_PREFIX. Se você não definir o prefixo, o valor padrão na_bg_ será usado.

Plug-in para SAP ASE

Configurações de recursos:

- SYBASE_SERVER (data_server_name) especifica o nome do servidor de dados Sybase (opção -S no comando isql). Por exemplo, p_test.
- SYBASE_DATABASES_EXCLUDE (db_name) permite que bancos de dados sejam excluídos se a construção "ALL" for usada.

Você pode especificar vários bancos de dados usando uma lista separada por ponto e vírgula. Por exemplo: pubs2;test_db1.

- SYBASE_USER: user_name especifica o usuário do sistema operacional que pode executar o comando isql.

  Obrigatório para UNIX. Este parâmetro é necessário se o usuário que executa os comandos iniciar e parar do Snap Creator Agent (geralmente o usuário root) e o usuário que executa o comando isql forem diferentes.

- SYBASE_TRAN_DUMP db_name:directory_path permite que você execute um dump de transação do Sybase após criar um snapshot. Por exemplo, pubs2:/sybasedumps/ pubs2

  Você deve especificar cada banco de dados que requer um despejo de transação.

- SYBASE_TRAN_DUMP_COMPRESS (S|N) habilita ou desabilita a compactação de despejo de transações nativas do Sybase.
- SYBASE_ISQL_CMD (por exemplo, /opt/sybase/OCS-15_0/bin/isql) define o caminho para o comando isql.
- SYBASE_EXCLUDE_TEMPDB (S|N) permite que você exclua automaticamente bancos de dados temporários criados pelo usuário.

Plug-in para aplicativos Oracle (ORASCPM)

Configurações de recursos:

- SQLPLUS_CMD especifica o caminho para SQLplus.
- ORACLE_DATABASES lista os bancos de dados Oracle a serem copiados e o usuário correspondente (banco de dados:usuário).
- CNTL_FILE_BACKUP_DIR especifica o diretório para backup do arquivo de controle.
- ORA_TEMP especifica o diretório para arquivos temporários.
- ORACLE_HOME especifica o diretório onde o software Oracle está instalado.
- ARCHIVE_LOG_ONLY especifica se os logs de arquivamento devem ser feitos ou não.
- ORACLE_BACKUPMODE especifica se o backup deve ser executado online ou offline.
- ORACLE_EXPORT_PARAMETERS especifica se as variáveis de ambiente definidas acima devem ser reexportadas durante a execução de */bin/su <usuário executando sqlplus> -c sqlplus /nolog <cmd>*. Este é normalmente o caso quando o usuário que está executando o sqlplus não definiu todas as variáveis de ambiente necessárias para se conectar ao banco de dados usando *connect / as sysdba*.

Criar políticas para recursos de plug-in suportados NetApp

Antes de usar o SnapCenter para fazer backup de recursos específicos do plug-in suportados NetApp , você deve criar uma política de backup para o recurso ou grupo de recursos do qual deseja fazer backup.

Antes de começar

- Você deve ter definido sua estratégia de backup.

  Para obter detalhes, consulte as informações sobre como definir uma estratégia de proteção de dados para plug-ins compatíveis com NetApp .

- Você deveria estar preparado para a proteção de dados.

  A preparação para a proteção de dados inclui tarefas como instalar o SnapCenter, adicionar hosts, criar conexões de sistema de armazenamento e adicionar recursos.

- As máquinas virtuais de armazenamento (SVMs) devem ser atribuídas a você para operações de espelhamento ou cofre.

  O administrador do SnapCenter deve ter atribuído as SVMs para os volumes de origem e destino a você se estiver replicando Snapshots para um espelho ou cofre.

- Você deve ter adicionado manualmente os recursos que deseja proteger.

Sobre esta tarefa

- Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e mantém backups. Além disso, você pode especificar configurações de replicação, script e aplicativo.
- Especificar opções em uma política economiza tempo quando você deseja reutilizar a política para outro grupo de recursos.
- SnapLock
  - Se a opção 'Manter as cópias de backup por um número específico de dias' for selecionada, o período de retenção do SnapLock deverá ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio de Snapshot impede a exclusão dos Snapshots até que o período de retenção expire. Isso pode levar à retenção de um número maior de Snapshots do que a contagem especificada na política.
  - Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

> As configurações primárias do SnapLock são gerenciadas na política de backup do SnapCenter e as configurações secundárias do SnapLock são gerenciadas pelo ONTAP.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Clique em **Novo**.
4. Na página Nome, insira o nome e os detalhes da política.
5. Na página Tipo de política, faça o seguinte:
   a. Selecione o tipo de armazenamento.
   b. Na seção Configurações de backup personalizadas, forneça quaisquer configurações de backup específicas que devem ser passadas ao plug-in no formato chave-valor.

      Você pode fornecer vários valores-chave a serem passados ao plug-in.

6. Na página Snapshot e Replicação, execute as seguintes etapas:

   a. Especifique o tipo de programação selecionando **Sob demanda**, **Por hora**, **Diário**, **Semanal** ou **Mensal**.

Você pode especificar o agendamento (data de início, data de término e frequência) para a operação de backup ao criar um grupo de recursos. Isso permite que você crie grupos de recursos que compartilham a mesma política e frequência de backup, mas permite que você atribua agendamentos de backup diferentes a cada política.

Se você agendou para 2h00, a programação não será acionada durante o horário de verão (DST).

a. Na seção Configurações de instantâneo, especifique as configurações de retenção para o tipo de backup e o tipo de agendamento selecionado na página **Tipo de backup**:

Se você quiser…	**Então…**
Mantenha um certo número de Snapshots	Selecione **Cópias a serem mantidas** e especifique o número de Snapshots que você deseja manter. Se o número de Snapshots exceder o número especificado, os Snapshots serão excluídos, com as cópias mais antigas sendo excluídas primeiro. Você deve definir a contagem de retenção como 2 ou mais se planeja habilitar a replicação do SnapVault . Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro Snapshot será o Snapshot de referência para o relacionamento SnapVault até que um Snapshot mais recente seja replicado para o destino. O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida como um valor maior do que o suportado pela versão subjacente do ONTAP .
Mantenha os Snapshots por um certo número de dias	Selecione **Manter cópias por** e especifique o número de dias pelos quais você deseja manter os Snapshots antes de excluí-los.
Período de bloqueio de cópia de instantâneo	Selecione **Período de bloqueio de cópia de instantâneo** e especifique dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

b. Selecione um rótulo de política.

> Você pode atribuir rótulos SnapMirror a snapshots primários para replicação remota, permitindo que os snapshots primários descarreguem a operação de replicação de snapshots do SnapCenter para sistemas secundários ONTAP . Isso pode ser feito sem habilitar a opção SnapMirror ou SnapVault na página de política.

7. Na seção Selecionar opções de replicação secundária, selecione uma ou ambas as seguintes opções de replicação secundária:

Para este campo…	Faça isso…
Atualize o SnapMirror após criar uma cópia local do Snapshot	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Se o relacionamento de proteção no ONTAP for do tipo Mirror and Vault e se você selecionar apenas esta opção, o Snapshot criado no primário não será transferido para o destino, mas será listado no destino. Se este Snapshot for selecionado no destino para executar uma operação de restauração, a seguinte mensagem de erro será exibida: O local secundário não está disponível para o backup em cofre/espelho selecionado. Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Ver "Exibir backups e clones relacionados a recursos de plug-ins suportados pela NetApp na página Topologia" .

Para este campo…	Faça isso…
Atualize o SnapVault após criar uma cópia local do Snapshot	Selecione esta opção para executar a replicação de backup de disco para disco (backups do SnapVault). Durante a replicação secundária, o tempo de expiração do SnapLock carrega o tempo de expiração do SnapLock primário. Clicar no botão **Atualizar** na página Topologia atualiza o tempo de expiração do SnapLock secundário e primário que são recuperados do ONTAP. Quando o SnapLock é configurado somente no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página Topologia atualiza o período de bloqueio no secundário recuperado do ONTAP. Para obter mais informações sobre o SnapLock Vault, consulte Confirmar instantâneos no WORM em um destino de cofre. Ver "Exibir backups e clones relacionados a recursos de plug-ins suportados pela NetApp na página Topologia" .
Erro na contagem de novas tentativas	Insira o número máximo de tentativas de replicação que podem ser permitidas antes que a operação seja interrompida.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o armazenamento secundário para evitar atingir o limite máximo de Snapshots no armazenamento secundário.

8. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas

Um grupo de recursos é o contêiner ao qual você deve adicionar recursos que deseja fazer backup e proteger. Ele permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que deseja executar.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione Novo grupo de recursos.
3. Na página Nome, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Insira um nome para o grupo de recursos. Observação: o nome do grupo de recursos não deve exceder 250 caracteres.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.
Use formato de nome personalizado para cópia do Snapshot	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot. Por exemplo, *customtext_resource group_policy_hostname ou resource group_hostname*. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

4. Opcional: Na página Recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Tipo de recurso**.

   Isso ajuda a filtrar informações na tela.

5. Selecione os recursos na seção **Recursos disponíveis** e, em seguida, selecione a seta para a direita para movê-los para a seção **Recursos selecionados**.
6. Opcional: Na página **Configurações do aplicativo**, faça o seguinte:

   a. Selecione a seta Backups para definir opções adicionais de backup:

      Habilite o backup do grupo de consistência e execute as seguintes tarefas:

Para este campo…	Faça isso…
Permitir tempo de espera para que a operação do Consistency Group Snapshot seja concluída	Selecione Urgente, Médio ou Relaxado para especificar o tempo de espera para a conclusão da operação de Snapshot. Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.
Desativar sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL .

+

a. Selecione a seta Scripts e insira os comandos pre e post para operações de inatividade, instantâneo e ativação/desativação. Você também pode inserir os pré-comandos a serem executados antes de sair em caso de falha.

b. Selecione a seta Configurações personalizadas e insira os pares de chave-valor personalizados necessários para todas as operações de proteção de dados que usam este recurso.

Parâmetro	Contexto	Descrição
HABILITAR_REGISTRO_DE_ARQUIVO	(S/N)	Permite que o gerenciamento de log de arquivamento exclua os logs de arquivamento.
RETENÇÃO_DE_REGISTRO_DE_ARQUIVO	número_de_dias	Especifica o número de dias que os logs de arquivamento são retidos. Esta configuração deve ser igual ou maior que NTAP_SNAPSHOT_RETENTIONS.
DIRETÓRIO_DE_LOG_DE_ARQUIVO	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs de arquivamento.

Parâmetro	Contexto	Descrição
EXT_DE_LOG_DE_ARQUIVO	extensão_de_arquivo	Especifica o comprimento da extensão do arquivo de log de arquivamento. Por exemplo, se o log de arquivamento for log_backup_0_0_0_0.16151855 1942 9 e se o valor file_extension for 5, a extensão do log manterá 5 dígitos, que é 16151.
ARQUIVO_LOG_RECURSIVO_ SE ARQUIVO	(S/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs de arquivamento estiverem localizados em subdiretórios.

c. Selecione a seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar Instantâneos:

Se você quiser…	Então…
SnapCenter para usar o plug-in para Windows e colocar o sistema de arquivos em um estado consistente antes de criar um Snapshot. Para recursos do Linux, esta opção não é aplicável.	Selecione * SnapCenter com consistência do sistema de arquivos*. Esta opção não é aplicável ao SnapCenter Plug-in para banco de dados SAP HANA.
SnapCenter para criar um instantâneo de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.
Para inserir o comando a ser executado no host para criar Snapshots.	Selecione **Outro** e insira o comando a ser executado no host para criar um Snapshot.

7. Na página Políticas, execute as seguintes etapas:

a. Selecione uma ou mais políticas na lista suspensa.

Você também pode criar uma política selecionando * + *.

As políticas estão listadas na seção **Configurar agendamentos para políticas selecionadas**.

b. Na coluna **Configurar agendamentos**, selecione * + * para a política que você deseja configurar.

c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione OK.

   Onde policy_name é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados. Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Na lista suspensa **Preferências de e-mail** na página **Notificação**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. O servidor SMTP deve ser configurado em **Configurações** > **Configurações globais**.

9. Revise o resumo e selecione **Concluir**.

Crie grupos de recursos e habilite proteção secundária para recursos em sistemas ASA r2

Você deve criar o grupo de recursos para adicionar os recursos que estão nos sistemas ASA r2. Você também pode provisionar a proteção secundária ao criar o grupo de recursos.

Antes de começar

- Você deve garantir que não está adicionando recursos do ONTAP 9.x e recursos do ASA r2 ao mesmo grupo de recursos.
- Você deve garantir que não tenha um banco de dados com recursos ONTAP 9.x e recursos ASA r2.

Sobre esta tarefa

- A proteção secundária estará disponível somente se o usuário conectado estiver atribuído à função que tem o recurso **SecondaryProtection** habilitado.
- Se você habilitar a proteção secundária, o grupo de recursos será colocado no modo de manutenção durante a criação dos grupos de consistência primário e secundário. Depois que os grupos de consistência primário e secundário são criados, o grupo de recursos é retirado do modo de manutenção.
- O SnapCenter não oferece suporte à proteção secundária para um recurso clone.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:
   a. Insira um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 caracteres.

   b. Insira um ou mais rótulos no campo Tag para ajudar você a pesquisar o grupo de recursos posteriormente.

      Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar posteriormente todos os grupos de recursos associados à tag RH.

c. Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

   Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

d. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

   Você deve usar exatamente o mesmo destino definido no aplicativo, incluindo o prefixo, se necessário.

4. Na página Recursos, selecione o nome do host do banco de dados na lista suspensa **Host**.

   Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos do ASA r2 na seção Recursos disponíveis e mova-os para a seção Recursos selecionados.
6. Na página Configurações do aplicativo, selecione a opção de backup.
7. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em + .

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

   c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

      Onde *policy_name* é o nome da política que você selecionou.

      Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

   Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Se a proteção secundária estiver habilitada para a política selecionada, a página Proteção Secundária será exibida e você precisará executar as seguintes etapas:

   a. Selecione o tipo de política de replicação.

      A política de replicação síncrona não é suportada.

   b. Especifique o sufixo do grupo de consistência que você deseja usar.

   c. Nos menus suspensos Cluster de destino e SVM de destino, selecione o cluster emparelhado e o SVM

que você deseja usar.

O cluster e o peering de SVM não são suportados pelo SnapCenter. Você deve usar o System Manager ou as CLIs do ONTAP para executar o peering de cluster e SVM.

Se os recursos já estiverem protegidos fora do SnapCenter, eles serão exibidos na seção Recursos Protegidos Secundários.

1. Na página Verificação, execute as seguintes etapas:
   a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para realizar a verificação no armazenamento secundário.
   b. Clique + na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política.
   c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name, execute as seguintes ações:

Se você quiser…	Faça isso…
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

   d. Selecione **Verificar no local secundário** para verificar seus backups no sistema de armazenamento secundário.
   e. Clique em **OK**.

   Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

2. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

   Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

3. Revise o resumo e clique em **Concluir**.

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell

Você deve criar uma conexão de máquina virtual de armazenamento (SVM) e uma credencial antes de usar cmdlets do PowerShell para executar operações de proteção de dados.

Antes de começar

- Você deve ter preparado o ambiente do PowerShell para executar os cmdlets do PowerShell.
- Você deve ter as permissões necessárias na função de administrador de infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estejam em andamento.

  As instalações do plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento porque o cache do host pode não ser atualizado e o status dos bancos de dados pode ser exibido na GUI do SnapCenter como “Não disponível para backup” ou "`Não no armazenamento NetApp ".

- Os nomes dos sistemas de armazenamento devem ser exclusivos.

  O SnapCenter não oferece suporte a vários sistemas de armazenamento com o mesmo nome em clusters diferentes. Cada sistema de armazenamento suportado pelo SnapCenter deve ter um nome exclusivo e um endereço IP LIF de gerenciamento exclusivo.

Passos

1. Inicie uma sessão de conexão do PowerShell Core usando o cmdlet Open-SmConnection.

   Este exemplo abre uma sessão do PowerShell:

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

2. Crie uma nova conexão com o sistema de armazenamento usando o cmdlet Add-SmStorageConnection.

   Este exemplo cria uma nova conexão de sistema de armazenamento:

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Crie uma nova credencial usando o cmdlet Add-SmCredential.

   Este exemplo cria uma nova credencial chamada FinanceAdmin com credenciais do Windows:

   ```
   PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Faça backup de recursos individuais de plug-ins suportados pela NetApp

Se um recurso de plug-in individual compatível com NetApp não fizer parte de nenhum grupo de recursos, você poderá fazer backup do recurso na página Recursos. Você pode

fazer backup do recurso sob demanda ou, se o recurso tiver uma política anexada e um agendamento configurado, os backups ocorrerão automaticamente de acordo com o agendamento.

Antes de começar

- Você deve ter criado uma política de backup.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Clique e selecione o nome do host e o tipo de recurso para filtrar os recursos. Você pode então clicar para fechar o painel de filtro.
3. Clique no recurso que você deseja fazer backup.
4. Na página Recurso, se desejar usar um nome personalizado, marque a caixa de seleção **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado para o nome do Snapshot.

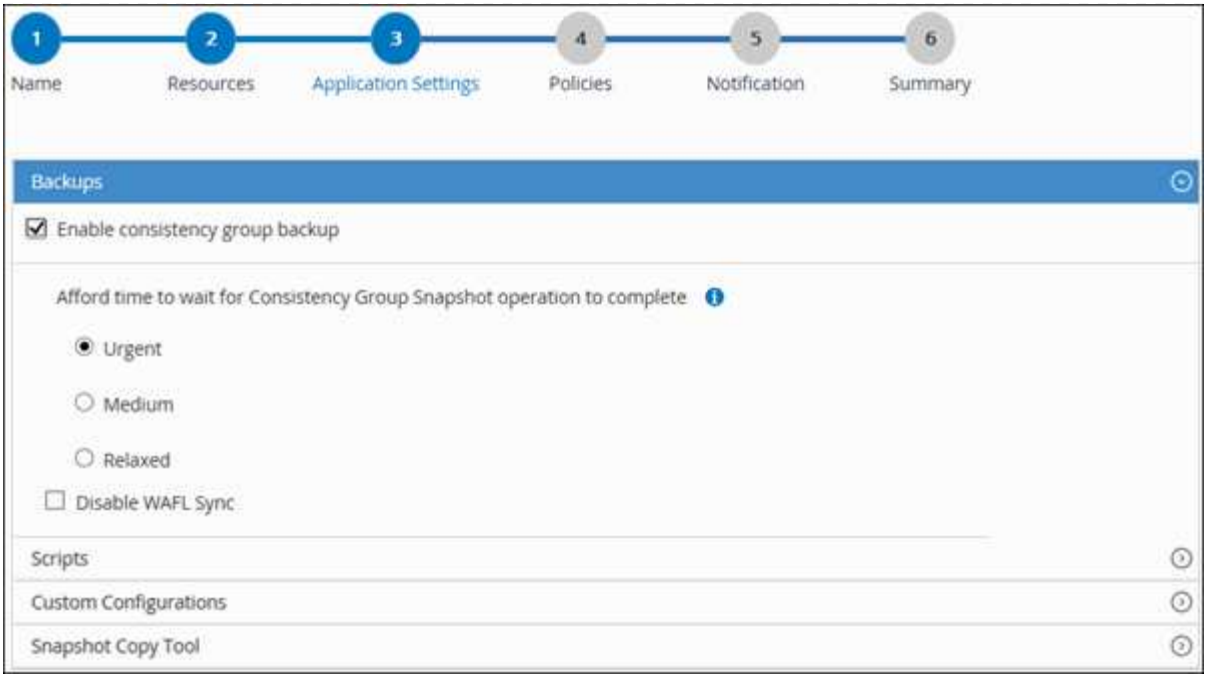
   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.
5. Na página Configurações do aplicativo, faça o seguinte:

   a. Clique na seta **Backups** para definir opções adicionais de backup:

      Habilite o backup do grupo de consistência, se necessário, e execute as seguintes tarefas:

Para este campo…	Faça isso…
Permitir tempo de espera para que a operação do Consistency Group Snapshot seja concluída	Selecione Urgente, Médio ou Relaxado para especificar o tempo de espera para a conclusão da operação de Snapshot. Urgente = 5 segundos, Médio = 7 segundos e Relaxado = 20 segundos.
Desativar sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL .

+



a. Clique na seta **Scripts** para executar comandos pré e pós para operações de inatividade, instantâneo e ativação/desativação. Você também pode executar pré-comandos antes de sair da operação de backup.

   Prescrições e pós-escritos são executados no SnapCenter Server.

b. Clique na seta **Configurações personalizadas** e insira os pares de valores personalizados necessários para todos os trabalhos que usam este recurso.

c. Clique na seta **Ferramenta de Cópia de Instantâneo** para selecionar a ferramenta para criar Instantâneos:

Se você quiser…	Então…
SnapCenter para tirar um instantâneo de nível de armazenamento	Selecione * SnapCenter sem consistência do sistema de arquivos*.
SnapCenter para usar o plug-in para Windows para colocar o sistema de arquivos em um estado consistente e, em seguida, tirar um instantâneo	Selecione * SnapCenter com consistência do sistema de arquivos*.
Para inserir o comando para criar um Snapshot	Selecione **Outro** e insira o comando para criar um Snapshot.

6. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

   Você também pode criar uma política clicando em + .

   Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são

listadas.

b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

Onde *policy_name* é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

7. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. O SMTP também deve ser configurado em **Configurações** > **Configurações globais**.

8. Revise o resumo e clique em **Concluir**.

A página de topologia de recursos é exibida.

9. Clique em **Fazer backup agora**.
10. Na página Backup, execute as seguintes etapas:

a. Se você aplicou várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

b. Clique em **Backup**.

11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-smconnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146\
```

O prompt de nome de usuário e senha é exibido.

2. Adicione recursos usando o cmdlet Add-SmResources.

Este exemplo adiciona recursos:

```
Add-SmResource -HostName 'scc55.sccore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_vol1_scc55_sccore_test_com";"QTREENAME"="qtree
Vol1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. Crie uma política de backup usando o cmdlet Add-SmPolicy.

   Este exemplo cria uma nova política de backup:

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'
-PluginPolicyType DummyPlugin  -description 'testPolicy'
```

4. Adicione um novo grupo de recursos ao SnapCenter usando o cmdlet Add-SmResourceGroup.

   Este exemplo cria um novo grupo de recursos com a política e os recursos especificados:

```
Add-SmResourceGroup -ResourceGroupName
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'
-Resources
@(@{"Host"="scc55.sccore.test.com";"Uid"="QTREE2";"PluginName"="Dumm
yPlugin"},@{"Host"="scc55.sccore.test.com";"Uid"="QTREE";"PluginName
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'
-usesnapcenterwithoutfilesystemconsistency
```

5. Inicie uma nova tarefa de backup usando o cmdlet New-SmBackup.

```
New-SMBackup -DatasetName
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy
test2
```

6. Visualize o status do trabalho de backup usando o cmdlet Get-SmBackupReport.

   Este exemplo exibe um relatório de resumo de todos os trabalhos que foram executados na data especificada:

```
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
```

Fazer backup de grupos de recursos de plug-ins suportados NetApp

Você pode fazer backup de um grupo de recursos sob demanda na página Recursos. Se um grupo de recursos tiver uma política anexada e um agendamento configurado, os backups ocorrerão automaticamente de acordo com o agendamento.

Antes de começar

- Você deve ter criado um grupo de recursos com uma política anexada.
- Se você quiser fazer backup de um recurso que tenha um relacionamento SnapMirror com o armazenamento secundário, a função ONTAP atribuída ao usuário do armazenamento deve incluir o

privilégio “snapmirror all”. Entretanto, se você estiver usando a função “vsadmin”, o privilégio “snapmirror all” não será necessário.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.

   Você pode pesquisar o grupo de recursos inserindo o nome do grupo de recursos na caixa de pesquisa ou clicando em e selecionando a tag. Você pode então clicar para fechar o painel de filtro.
3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e clique em **Fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
   a. Se você tiver associado várias políticas ao grupo de recursos, na lista suspensa **Política**, selecione a política que deseja usar para backup.

      Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

   b. Clique em **Backup**.
5. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.
   - Nas configurações do MetroCluster , o SnapCenter pode não conseguir detectar um relacionamento de proteção após um failover.

     "Não é possível detectar o relacionamento SnapMirror ou SnapVault após failover do MetroCluster"
   - Se você estiver fazendo backup de dados do aplicativo em VMDKs e o tamanho do heap Java para o SnapCenter Plug-in for VMware vSphere não for grande o suficiente, o backup poderá falhar. Para aumentar o tamanho do heap Java, localize o arquivo de script /opt/netapp/init_scripts/scvservice. Nesse roteiro, o `do_start method` O comando inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: `Java -jar -Xmx8192M -Xms4096M`.

Monitorar operações de backup de recursos de plug-in com suporte da NetApp

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Talvez você queira verificar o progresso para determinar quando ele foi concluído ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado correspondente das operações:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **Trabalhos**.
3. Na página Trabalhos, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de backup sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Backup**.
   d. No menu suspenso **Status**, selecione o status do backup.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione uma tarefa de backup e clique em **Detalhes** para visualizar os detalhes da tarefa.

   Embora o status do trabalho de backup seja exibido , ao clicar em detalhes do trabalho, você poderá ver que algumas das tarefas filhas da operação de backup ainda estão em andamento ou marcadas com sinais de alerta.

5. Na página Detalhes do trabalho, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Cancelar operações de backup para plug-ins compatíveis com NetApp

Você pode cancelar operações de backup que estão na fila.

O que você vai precisar

- Você deve estar conectado como administrador do SnapCenter ou proprietário do trabalho para cancelar operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **Atividade**.
- Não é possível cancelar uma operação de backup em execução.
- Você pode usar a GUI do SnapCenter , os cmdlets do PowerShell ou os comandos da CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** fica desabilitado para operações que não podem ser canceladas.
- Se você selecionou **Todos os membros desta função podem ver e operar em objetos de outros membros** na página Usuários\Grupos ao criar uma função, você pode cancelar as operações de backup enfileiradas de outros membros enquanto estiver usando essa função.

Passos

1. Execute uma das seguintes ações:

Do…	Ação
Página do monitor	a. No painel de navegação esquerdo, clique em **Monitor** > **Trabalhos**. b. Selecione a operação e clique em **Cancelar trabalho**.
Painel de atividades	a. Após iniciar a operação de backup, clique em * * no painel Atividade para visualizar as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes do trabalho, clique em **Cancelar trabalho**.

A operação é cancelada e o recurso é revertido ao estado anterior.

Exibir backups e clones relacionados a recursos de plug-ins suportados pela NetApp na página Topologia

Ao se preparar para fazer backup ou clonar um recurso, pode ser útil visualizar uma representação gráfica de todos os backups e clones no armazenamento primário e secundário. Na página Topologia, você pode ver todos os backups e clones disponíveis para o recurso ou grupo de recursos selecionado. Você pode visualizar os detalhes desses backups e clones e selecioná-los para executar operações de proteção de dados.

Sobre esta tarefa

Você pode revisar os seguintes ícones na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no armazenamento primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups e clones que estão disponíveis no armazenamento primário.
- exibe o número de backups e clones que são espelhados no armazenamento secundário usando a tecnologia SnapMirror .

  Clones de um backup de um espelho flexível em termos de versão em um volume do tipo mirror-vault são exibidos na exibição de topologia, mas a contagem de backups de espelho na exibição de topologia não inclui o backup flexível em termos de versão.

- exibe o número de backups e clones que são replicados no armazenamento secundário usando a tecnologia SnapVault .

  O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo,

se você criou 6 backups usando uma política para manter apenas 4 backups, o número de backups exibidos será 6.

Clones de um backup de um espelho flexível em termos de versão em um volume do tipo mirror-vault são exibidos na exibição de topologia, mas a contagem de backups de espelho na exibição de topologia não inclui o backup flexível em termos de versão.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso na exibição de detalhes do recurso ou na exibição de detalhes do grupo de recursos.

   Se o recurso estiver protegido, a página de topologia do recurso selecionado será exibida.

4. Revise o cartão Resumo para ver um resumo do número de backups e clones disponíveis no armazenamento primário e secundário.

   A seção Cartão de Resumo exibe o número total de backups e clones.

   Clicar no botão de atualização inicia uma consulta ao armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clicar no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Uma programação semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo estiver distribuído em vários volumes, o tempo de expiração do SnapLock para o backup será o maior tempo de expiração do SnapLock definido para um Snapshot em um volume. O maior tempo de expiração do SnapLock é recuperado do ONTAP.

   Após o backup sob demanda, clicar no botão **Atualizar** atualiza os detalhes do backup ou clone.

5. Na exibição Gerenciar cópias, clique em **Backups** ou **Clones** do armazenamento primário ou secundário para ver detalhes de um backup ou clone.

   Os detalhes dos backups e clones são exibidos em formato de tabela.

6. Selecione o backup na tabela e clique nos ícones de proteção de dados para executar operações de restauração, clonagem, renomeação e exclusão.

   Não é possível renomear ou excluir backups que estejam no sistema de armazenamento secundário.

   Não é possível renomear os backups que estão no sistema de armazenamento primário.

7. Se você quiser excluir um clone, selecione o clone da tabela e clique em para excluir o clone.

Restaurar recursos de plug-ins suportados pela NetApp

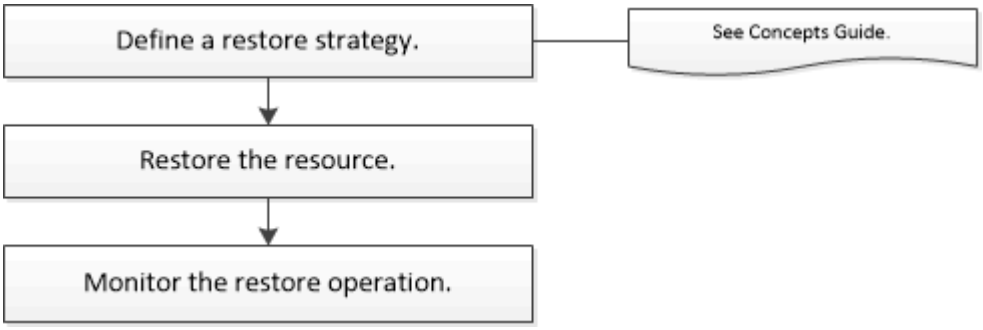
Restaurar recursos de plug-in suportados pelo NetApp

O fluxo de trabalho de restauração e recuperação inclui planejamento, execução de

operações de restauração e monitoramento das operações.

Sobre esta tarefa

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de restauração:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. Para obter informações sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte o "Guia de referência do cmdlet do software SnapCenter" .

Restaurar um backup de recurso

Você pode usar o SnapCenter para restaurar recursos. Os recursos das operações de restauração dependem do plug-in que você usa.

Antes de começar

- Você deve ter feito backup do recurso ou dos grupos de recursos.
- O administrador do SnapCenter deve ter atribuído a você as máquinas virtuais de armazenamento (SVMs) para os volumes de origem e de destino se você estiver replicando Snapshots para um espelho ou cofre.
- Você deve ter cancelado qualquer operação de backup que esteja em andamento para o recurso ou grupo de recursos que deseja restaurar.

Sobre esta tarefa

- A operação de restauração padrão restaura apenas objetos de armazenamento. As operações de restauração no nível do aplicativo só poderão ser executadas se o plug-in compatível com NetApp fornecer esse recurso.
- Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com informações como tipo, nome do host ou cluster, grupos de recursos e políticas associados e status.

   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

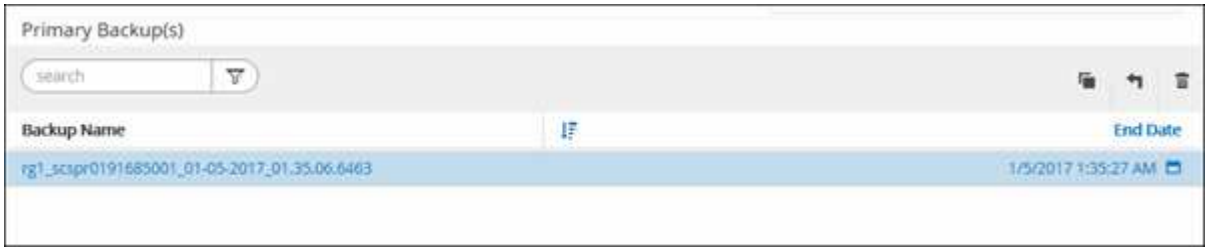
   Se o recurso não estiver protegido, *Não protegido* será exibido na coluna **Status geral**.

   O status *Não protegido* na coluna **Status geral** pode significar que o recurso não está protegido ou que o recurso foi feito backup por um usuário diferente.

3. Selecione o recurso ou selecione um grupo de recursos e, em seguida, selecione um recurso nesse grupo.

   A página de topologia de recursos é exibida.

4. Na exibição **Gerenciar cópias**, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela de backup(s) primário(s), selecione o backup que deseja restaurar e clique em .



6. Na página Escopo de restauração, selecione **Recurso completo** ou **Nível de arquivo**.
   a. Se você selecionou **Recurso Completo**, o backup do recurso será restaurado.

      Se o recurso contiver volumes ou qtrees como Storage Footprint, os Snapshots mais recentes nesses volumes ou qtrees serão excluídos e não poderão ser recuperados. Além disso, se qualquer outro recurso estiver hospedado nos mesmos volumes ou qtrees, esse recurso também será excluído.

   b. Se você selecionou **Nível de arquivo**, poderá selecionar **Todos** ou selecionar volumes ou qtrees e, em seguida, inserir o caminho relacionado aos volumes ou qtrees selecionados, separados por vírgulas.
      - Você pode selecionar vários volumes e qtrees.
      - Se o tipo de recurso for LUN, o LUN inteiro será restaurado. Você pode selecionar vários LUNs. + NOTA: Se você selecionar **Todos**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.
7. Na página **Pré-operações**, insira os comandos pre restore e unmount para executar antes de

realizar um trabalho de restauração.

8. Na página **Post ops**, insira os comandos mount e post restore para serem executados após realizar um trabalho de restauração.
9. Na página **Notificação**, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. O SMTP também deve ser configurado na página **Configurações** > **Configurações globais**.

10. Revise o resumo e clique em **Concluir**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

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

2. Recupere as informações sobre um ou mais backups que você deseja restaurar usando os cmdlets Get-SmBackup e Get-SmBackupReport.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
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
```

   Este exemplo exibe informações detalhadas sobre o backup de 29 de janeiro de 2015 a 3 de fevereiro de 2015:

```
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. Restaure os dados do backup usando o cmdlet Restore-SmBackup.

```
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          :
```

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Monitorar operações de restauração de recursos de plug-in suportados NetApp

Você pode monitorar o progresso de diferentes operações de restauração do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa tomar.

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de restauração sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Restaurar**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Aplicar** para visualizar as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Clonar backups de recursos de plug-ins suportados pelo NetApp

Clonar backups de recursos de plug-ins suportados pelo NetApp

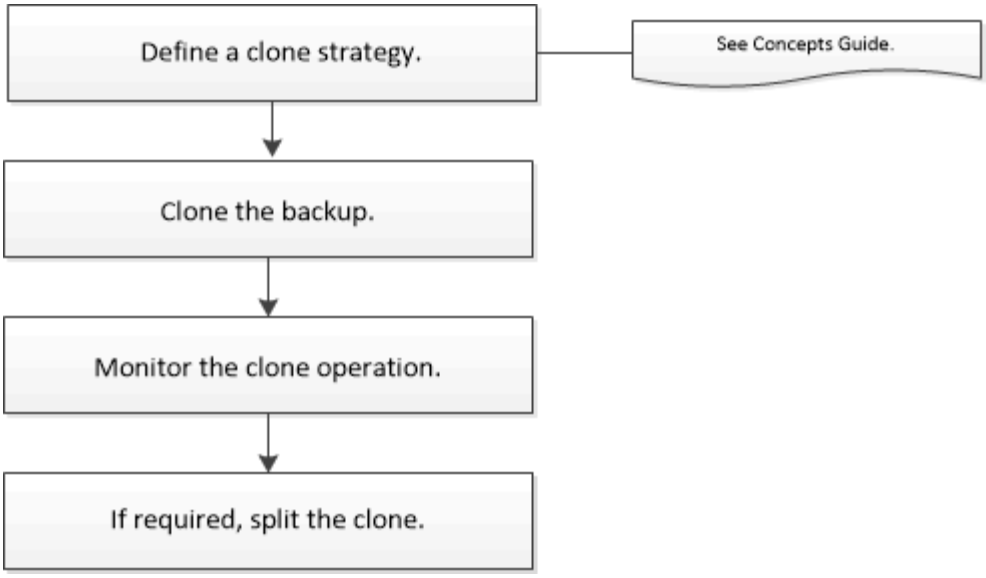
O fluxo de trabalho de clonagem inclui executar a operação de clonagem e monitorar a operação.

Sobre esta tarefa

Você pode clonar backups de recursos pelos seguintes motivos:

- Para testar a funcionalidade que deve ser implementada usando a estrutura e o conteúdo atuais dos recursos durante os ciclos de desenvolvimento do aplicativo
- Para ferramentas de extração e manipulação de dados ao preencher data warehouses
- Para recuperar dados que foram excluídos ou alterados por engano

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar a operação de clonagem:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clonagem. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet do SnapCenter ou consulte o "Guia de referência do cmdlet do software SnapCenter" .

Clonar de um backup

Você pode usar o SnapCenter para clonar um backup. Você pode clonar a partir do backup primário ou secundário. Os recursos das operações de clonagem dependem do plug-in que você usa.

Antes de começar

- Você deve ter feito backup dos recursos ou do grupo de recursos.
- A operação de clonagem padrão clona apenas objetos de armazenamento. As operações de clonagem no nível do aplicativo só podem ser executadas se o plug-in compatível com o NetApp fornecer esse recurso.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de armazenamento (SVM).

Sobre esta tarefa

Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Interface do usuário do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página **Recursos**, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos junto com informações como tipo, nome do host ou cluster, grupos de recursos e políticas associados e status.

3. Selecione o recurso ou grupo de recursos.

   Você deve selecionar um recurso se selecionar um grupo de recursos.

   A página de topologia de recurso ou grupo de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Selecione o backup de dados da tabela e clique em  .
6. Na página Locais, faça o seguinte:

Para este campo…	Faça isso…
Servidor clone	Por padrão, o host de origem é preenchido. Se você quiser especificar um host diferente, selecione o host no qual o clone deve ser montado e o plug-in será instalado.
Sufixo clone	Isso é obrigatório quando o destino do clone é o mesmo que a origem. Insira um sufixo que será anexado ao nome do recurso recém-clonado. O sufixo garante que o recurso clonado seja exclusivo no host. Por exemplo, rs1_clone. Se você estiver clonando para o mesmo host do recurso original, deverá fornecer um sufixo para diferenciar o recurso clonado do recurso original; caso contrário, a operação falhará.

   Se o recurso selecionado for um LUN e você estiver clonando de um backup secundário, os volumes de destino serão listados. Uma única origem pode ter vários volumes de destino.

7. Na página **Configurações**, faça o seguinte:

Para este campo…	Faça isso…
Nome do iniciador	Digite o nome do iniciador do host, que pode ser um IQDN ou WWPN.

Para este campo…	Faça isso…
Protocolo Igroup	Selecione o protocolo Igroup.

A página de configurações será exibida somente se o tipo de armazenamento for LUN.

8. Na página Scripts, insira os comandos para pré-clonagem ou pós-clonagem que devem ser executados antes ou depois da operação de clonagem, respectivamente. Digite o comando mount para montar um sistema de arquivos em um host.

   Por exemplo:

   - Comando pré-clone: exclui bancos de dados existentes com o mesmo nome
   - Comando post clone: verifica um banco de dados ou inicia um banco de dados.

     Comando de montagem para um volume ou qtree em uma máquina Linux: mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>

9. Na página **Notificação**, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail.

10. Revise o resumo e clique em **Concluir**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o SnapCenter Server para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

2. Liste os backups que podem ser clonados usando o cmdlet Get-SmBackup ou Get-SmResourceGroup.

   Este exemplo exibe informações sobre todos os backups disponíveis:

```
 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
```

Este exemplo exibe informações sobre um grupo de recursos especificado:

```
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                    : {}
    HostResourceMaping          : {}
    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                    : {}
    HostResourceMaping          : {}
    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. Inicie uma operação de clonagem de um grupo de recursos de clonagem ou de um backup existente usando o cmdlet New-SmClone.

   Este exemplo cria um clone de um backup especificado com todos os logs:

```
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. Visualize o status do trabalho de clonagem usando o cmdlet Get-SmCloneReport.

   Este exemplo exibe um relatório de clone para o ID do trabalho especificado:

```
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          :
```

Monitorar operações de clonagem de recursos de plug-in com suporte do NetApp

Você pode monitorar o progresso das operações de clonagem do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.

3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique  para filtrar a lista de modo que somente operações de clonagem sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione o trabalho de clonagem e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página Detalhes do trabalho, clique em **Exibir registros**.

Proteja os sistemas de arquivos Unix

O que você pode fazer com o plug-in SnapCenter para sistemas de arquivos Unix

Quando o Plug-in para sistemas de arquivos Unix estiver instalado em seu ambiente, você poderá usar o SnapCenter para fazer backup, restaurar e clonar sistemas de arquivos Unix. Você também pode executar tarefas de suporte a essas operações.

- Descubra recursos
- Fazer backup de sistemas de arquivos Unix
- Agendar operações de backup
- Restaurar backups do sistema de arquivos
- Backups do sistema de arquivos clone
- Monitore operações de backup, restauração e clonagem

Configurações suportadas

Item	Configuração suportada
Ambientes	• Servidor físico • Servidor virtual Datastores vVol em NFS e SAN. O datastore vVol só pode ser provisionado com o ONTAP Tools para VMware vSphere.
Sistemas operacionais	• Red Hat Enterprise Linux • Oracle Linux • Servidor SUSE Linux Enterprise (SLES)
Sistemas de arquivos	• SAN: ◦ Sistemas de arquivos baseados em LVM e não baseados em LVM ◦ LVM sobre VMDK ext3, ext4 e xfs • NFS: NFS v3, NFS v4.x
Protocolos	• FC • FCoE • iSCSI • NFS

Item	Configuração suportada
Multicaminho	sim

Limitações

- A combinação de RDMs e discos virtuais em um grupo de volumes não é suportada.
- A restauração em nível de arquivo não é suportada.

  No entanto, você pode executar manualmente a restauração no nível do arquivo clonando o backup e depois copiando os arquivos manualmente.

- A mistura de sistemas de arquivos distribuídos entre VMDKs provenientes de armazenamentos de dados NFS e VMFS não é suportada.
- NVMe não é suportado.
- O provisionamento não é suportado.

Características

- Permite que o plug-in para Oracle Database execute operações de proteção de dados em bancos de dados Oracle, manipulando a pilha de armazenamento do host subjacente em sistemas Linux ou AIX
- Suporta protocolos de Network File System (NFS) e de rede de área de armazenamento (SAN) em um sistema de armazenamento que esteja executando o ONTAP.
- Para sistemas Linux, os bancos de dados Oracle em LUNs VMDK e RDM são suportados quando você implanta o SnapCenter Plug-in for VMware vSphere e registra o plug-in com o SnapCenter.
- Suporta Mount Guard para AIX em sistemas de arquivos SAN e layout LVM.
- Suporta Enhanced Journaled File System (JFS2) com registro em linha em sistemas de arquivos SAN e layout LVM somente para sistemas AIX.

  Dispositivos nativos SAN, sistemas de arquivos e layouts LVM criados em dispositivos SAN são suportados.

- Automatiza operações de backup, restauração e clonagem com reconhecimento de aplicativo para sistemas de arquivos UNIX em seu ambiente SnapCenter

Instalar o plug-in SnapCenter para sistemas de arquivos Unix

Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Linux

Antes de adicionar um host e instalar o pacote de plug-ins para Linux, você deve atender a todos os requisitos.

- Se você estiver usando iSCSI, o serviço iSCSI deverá estar em execução.
- Você pode usar a autenticação baseada em senha para o usuário root ou não root ou a autenticação baseada em chave SSH.

  O plug-in SnapCenter para sistemas de arquivos Unix pode ser instalado por um usuário não root. No

entanto, você deve configurar os privilégios sudo para que o usuário não root instale e inicie o processo do plug-in. Após instalar o plug-in, os processos serão executados como um usuário não root.

- Crie credenciais com modo de autenticação como Linux para o usuário de instalação.
- Você deve ter instalado o Java 11 no seu host Linux.

  Certifique-se de ter instalado apenas a edição certificada do JAVA 11 no host Linux.

  Para obter informações sobre como baixar o JAVA, consulte: "Downloads Java para todos os sistemas operacionais"

- Você deve ter **bash** como o shell padrão para instalação de plug-ins.

Requisitos do host Linux

Você deve garantir que o host atenda aos requisitos antes de instalar o Pacote de plug-ins do SnapCenter para Linux.

Item	Requisitos
Sistemas operacionais	• Red Hat Enterprise Linux • Oracle Linux • Servidor SUSE Linux Enterprise (SLES)
RAM mínima para o plug-in SnapCenter no host	2 GB
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	2 GB Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.

Item	Requisitos
Pacotes de software necessários	Java 11 Oracle Java e OpenJDK Certifique-se de ter instalado apenas a edição certificada do JAVA 11 no host Linux. Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em /var/opt/snapcenter/spl/etc/spl.properties esteja definida para a versão correta do JAVA e o caminho correto.

Para obter as informações mais recentes sobre as versões suportadas, consulte o "Ferramenta de Matriz de Interoperabilidade da NetApp" .

Adicionar hosts e instalar o pacote de plug-ins para Linux usando a GUI

Você pode usar a página Adicionar Host para adicionar hosts e, em seguida, instalar o Pacote de Plug-ins do SnapCenter para Linux. Os plug-ins são instalados automaticamente nos hosts remotos.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Clique em **Adicionar**.
4. Na página Hosts, execute as seguintes ações:

Para este campo…	Faça isso…
Tipo de host	Selecione **Linux** como o tipo de host.
Nome do host	Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o FQDN. Se você estiver adicionando um host usando o SnapCenter e o host fizer parte de um subdomínio, você deverá fornecer o FQDN.

Para este campo…	Faça isso…
Credenciais	Selecione o nome da credencial que você criou ou crie novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais. Você pode visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou. O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar Host.

5. Na seção Selecionar plug-ins para instalar, selecione **Sistemas de arquivos Unix**.
6. (Opcional) Clique em **Mais opções**.

Para este campo…	Faça isso…
Porta	Mantenha o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão. Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.
Caminho de instalação	O caminho padrão é */opt/ NetApp/snapcenter*. Opcionalmente, você pode personalizar o caminho. Se você usar o caminho personalizado, certifique-se de que o conteúdo padrão dos sudoers seja atualizado com o caminho personalizado.
Ignorar verificações de pré-instalação opcionais	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.

7. Clique em **Enviar**.

Se você não tiver marcado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar

se ele atende aos requisitos para instalar o plug-in.

> O script de pré-verificação não valida o status do firewall da porta do plug-in se ele estiver especificado nas regras de rejeição do firewall.

Mensagens de erro ou aviso apropriadas serão exibidas se os requisitos mínimos não forem atendidos. Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em *C:\Program Files\ NetApp\ SnapCenter WebApp* para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.

> Em uma configuração de HA, se você estiver atualizando o arquivo web.config, deverá atualizar o arquivo em ambos os nós.

8. Verifique a impressão digital e clique em **Confirmar e Enviar**.

> O SnapCenter não suporta o algoritmo ECDSA.

> A verificação de impressão digital é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitore o progresso da instalação.

   Os arquivos de log específicos da instalação estão localizados em */custom_location/snapcenter/logs*.

Resultado

Todos os sistemas de arquivos montados no host são descobertos automaticamente e exibidos na Página de Recursos. Se nada for exibido, clique em **Atualizar recursos**.

Monitorar o status da instalação

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.

3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
   a. Clique em **Filtrar**.
   b. Opcional: especifique a data de início e término.
   c. No menu suspenso Tipo, selecione **Instalação de plug-in**.
   d. No menu suspenso Status, selecione o status da instalação.
   e. Clique em **Aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

Configurar o serviço SnapCenter Plug-in Loader

O serviço SnapCenter Plug-in Loader carrega o pacote de plug-in para Linux interagir com o SnapCenter Server. O serviço SnapCenter Plug-in Loader é instalado quando você instala o SnapCenter Plug-ins Package para Linux.

Sobre esta tarefa

Após instalar o pacote de plug-ins do SnapCenter para Linux, o serviço SnapCenter Plug-in Loader é iniciado automaticamente. Se o serviço SnapCenter Plug-in Loader não iniciar automaticamente, você deve:

- Certifique-se de que o diretório onde o plug-in está operando não seja excluído
- Aumentar o espaço de memória alocado à Máquina Virtual Java

O arquivo spl.properties, localizado em */custom_location/ NetApp/snapcenter/spl/etc/*, contém os seguintes parâmetros. Valores padrão são atribuídos a esses parâmetros.

Nome do parâmetro	Descrição
NÍVEL_LOG	Exibe os níveis de log suportados. Os valores possíveis são TRACE, DEBUG, INFO, WARN, ERROR e FATAL.
PROTOCOLO_SPL	Exibe o protocolo suportado pelo SnapCenter Plug-in Loader. Somente o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver faltando.
PROTOCOLO_DO_SERVIDOR_SNAPCENTER	Exibe o protocolo suportado pelo SnapCenter Server. Somente o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver faltando.

Nome do parâmetro	Descrição
PULAR_ATUALIZAÇÃO_JAVAHOME	Por padrão, o serviço SPL detecta o caminho Java e atualiza o parâmetro JAVA_HOME. Portanto, o valor padrão é definido como FALSE. Você pode definir como TRUE se quiser desabilitar o comportamento padrão e corrigir manualmente o caminho Java.
SPL_KEYSTORE_SENHA	Exibe a senha do arquivo keystore. Você só poderá alterar esse valor se alterar a senha ou criar um novo arquivo de keystore.
PORTA SPL	Exibe o número da porta na qual o serviço SnapCenter Plug-in Loader está em execução. Você pode adicionar o valor se o valor padrão estiver faltando. Você não deve alterar o valor após instalar os plug-ins.
SNAPCENTER_SERVER_HOST	Exibe o endereço IP ou nome do host do SnapCenter Server.
CAMINHO_DE_KEYSTORE_SPL	Exibe o caminho absoluto do arquivo keystore.
PORTA_DO_SERVIDOR_SNAPCENTER	Exibe o número da porta na qual o SnapCenter Server está sendo executado.
CONTAGEM_MÁXIMA_DE_LOGS	Exibe o número de arquivos de log do SnapCenter Plug-in Loader que são retidos na pasta */custom_location/snapcenter/spl/logs*. O valor padrão é definido como 5000. Se a contagem for maior que o valor especificado, os últimos 5000 arquivos modificados serão retidos. A verificação do número de arquivos é feita automaticamente a cada 24 horas a partir do momento em que o serviço SnapCenter Plug-in Loader é iniciado. Se você excluir manualmente o arquivo spl.properties, o número de arquivos a serem retidos será definido como 9999.

Nome do parâmetro	Descrição
JAVA_HOME	Exibe o caminho absoluto do diretório do JAVA_HOME que é usado para iniciar o serviço SPL. Este caminho é determinado durante a instalação e como parte do início do SPL.
TAMANHO_MÁXIMO_DE_LOG	Exibe o tamanho máximo do arquivo de log do trabalho. Quando o tamanho máximo é atingido, o arquivo de log é compactado e os logs são gravados no novo arquivo daquele trabalho.
RETER_REGISTROS_DOS_ÚLTIMOS_DIAS	Exibe o número de dias até os quais os logs são retidos.
HABILITAR_VALIDAÇÃO_DE_CERTIFICADO	Exibe verdadeiro quando a validação do certificado CA está habilitada para o host. Você pode habilitar ou desabilitar esse parâmetro editando o spl.properties ou usando a GUI ou o cmdlet do SnapCenter .

Se algum desses parâmetros não estiver atribuído ao valor padrão ou se você quiser atribuir ou alterar o valor, você poderá modificar o arquivo spl.properties. Você também pode verificar o arquivo spl.properties e editá-lo para solucionar quaisquer problemas relacionados aos valores atribuídos aos parâmetros. Depois de modificar o arquivo spl.properties, você deve reiniciar o serviço SnapCenter Plug-in Loader .

Passos

1. Execute uma das seguintes ações, conforme necessário:
   - Inicie o serviço SnapCenter Plug-in Loader :
     - Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - Pare o serviço SnapCenter Plug-in Loader :
     - Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     > Você pode usar a opção -force com o comando stop para interromper o serviço SnapCenter Plug-in Loader à força. No entanto, você deve ter cuidado antes de fazer isso, pois isso também encerra as operações existentes.

   - Reinicie o serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`

◦ Encontre o status do serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
- Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`

◦ Encontre a alteração no serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
- Como usuário não root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configurar certificado CA com o serviço SnapCenter Plug-in Loader (SPL) no host Linux

Você deve gerenciar a senha do keystore SPL e seu certificado, configurar o certificado CA, configurar certificados raiz ou intermediários para o trust-store SPL e configurar o par de chaves assinadas pela CA para o trust-store SPL com o serviço SnapCenter Plug-in Loader para ativar o certificado digital instalado.

O SPL usa o arquivo 'keystore.jks', que está localizado em '/var/opt/snapcenter/spl/etc' como seu armazenamento confiável e armazenamento de chaves.

Gerenciar senha para keystore SPL e alias do par de chaves assinadas pela CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore SPL a partir do arquivo de propriedades SPL.

   É o valor correspondente à chave 'SPL_KEYSTORE_PASS'.

2. Alterar a senha do keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Altere a senha de todos os aliases de entradas de chave privada no
keystore para a mesma senha usada para o keystore:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

   Atualize o mesmo para a chave SPL_KEYSTORE_PASS no arquivo spl.properties.

3. Reinicie o serviço após alterar a senha.

A senha para o keystore SPL e para todas as senhas de alias associadas da chave privada deve ser a mesma.

Configurar certificados raiz ou intermediários para armazenamento confiável SPL

Você deve configurar os certificados raiz ou intermediários sem a chave privada para o armazenamento confiável SPL.

Passos

1. Navegue até a pasta que contém o keystore SPL: */var/opt/snapcenter/spl/etc*.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

```
 keytool -list -v -keystore keystore.jks
. Adicione um certificado raiz ou intermediário:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Reinicie o serviço após configurar os certificados raiz ou
intermediários para o armazenamento confiável SPL.
```

Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

Configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL

Você deve configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL.

Passos

1. Navegue até a pasta que contém o keystore do SPL /var/opt/snapcenter/spl/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

```
 keytool -list -v -keystore keystore.jks
. Adicione o certificado da CA com chave privada e pública.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Listar os certificados adicionados no keystore.
```

```
 keytool -list -v -keystore keystore.jks
. Verifique se o keystore contém o alias correspondente ao novo
certificado CA, que foi adicionado ao keystore.
. Altere a senha da chave privada adicionada para o certificado CA para
a senha do keystore.
```

A senha padrão do keystore SPL é o valor da chave SPL_KEYSTORE_PASS no arquivo spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Se o nome do alias no certificado da CA for longo e contiver espaços
ou caracteres especiais ("*",","), altere o nome do alias para um nome
simples:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configure o nome do alias do keystore localizado no arquivo
spl.properties.
```

Atualize este valor em relação à chave SPL_CERTIFICATE_ALIAS.

4. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL.

Configurar lista de revogação de certificados (CRL) para SPL

Você deve configurar o CRL para SPL

Sobre esta tarefa

- O SPL procurará os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL do SPL é */var/opt/snapcenter/spl/etc/crl*.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo spl.properties com a chave SPL_CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

   Os certificados recebidos serão verificados em relação a cada CRL.

Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet run *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando *Get-SmCertificateSettings*.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- *  * indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- *  * indica que o certificado CA foi validado com sucesso.
- *  * indica que o certificado CA não pôde ser validado.
- *  * indica que as informações de conexão não puderam ser recuperadas.

Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

Instalar o SnapCenter Plug-in for VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs), ou se você quiser proteger VMs e armazenamentos de dados, será necessário implantar o SnapCenter Plug-in for VMware vSphere .

Para obter informações sobre como implantar, consulte "Visão geral da implantação" .

Implantar certificado CA

Para configurar o Certificado CA com o SnapCenter Plug-in for VMware vSphere, consulte "Criar ou importar certificado SSL" .

Configurar o arquivo CRL

O SnapCenter Plug-in for VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL do SnapCenter Plug-in for VMware vSphere é */opt/netapp/config/crl*.

Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Prepare-se para proteger sistemas de arquivos Unix

Antes de executar qualquer operação de proteção de dados, como operações de backup, clonagem ou restauração, você deve configurar seu ambiente. Você também pode configurar o SnapCenter Server para usar a tecnologia SnapMirror e SnapVault .

Para aproveitar a tecnologia SnapVault e SnapMirror , você deve configurar e inicializar um relacionamento de proteção de dados entre os volumes de origem e destino no dispositivo de armazenamento. Você pode usar o NetAppSystem Manager ou usar a linha de comando do console de armazenamento para executar essas tarefas.

Antes de usar o Plug-in para sistemas de arquivos Unix, o administrador do SnapCenter deve instalar e configurar o SnapCenter Server e executar as tarefas de pré-requisito.

- Instalar e configurar o SnapCenter Server."Saber mais"
- Configure o ambiente SnapCenter adicionando conexões do sistema de armazenamento."Saber mais"

> O SnapCenter não oferece suporte a várias SVMs com o mesmo nome em clusters diferentes. Cada SVM registrado no SnapCenter usando registro de SVM ou registro de cluster deve ser exclusivo.

- Adicione hosts, instale os plug-ins e descubra os recursos.
- Se você estiver usando o SnapCenter Server para proteger sistemas de arquivos Unix que residem em LUNs ou VMDKs do VMware RDM, será necessário implantar o SnapCenter Plug-in for VMware vSphere e registrar o plug-in no SnapCenter.
- Instale o Java no seu host Linux.
- Configure o SnapMirror e o SnapVault no ONTAP, se desejar replicação de backup.

Fazer backup de sistemas de arquivos Unix

Descubra os sistemas de arquivos UNIX disponíveis para backup

Após instalar o plug-in, todos os sistemas de arquivos naquele host são descobertos automaticamente e exibidos na página Recursos. Você pode adicionar esses sistemas de arquivos a grupos de recursos para executar operações de proteção de dados.

Antes de começar

- Você deve ter concluído tarefas como instalar o SnapCenter Server, adicionar hosts e criar conexões do sistema de armazenamento.
- Se os sistemas de arquivos residirem em um disco de máquina virtual (VMDK) ou mapeamento de dispositivo bruto (RDM), você deverá implantar o SnapCenter Plug-in for VMware vSphere e registrar o

plug-in com o SnapCenter.

Para obter mais informações, consulte "Implantar o SnapCenter Plug-in for VMware vSphere" .

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Caminho** na lista Exibir.
3. Clique em **Atualizar recursos**.

   Os sistemas de arquivos são exibidos junto com informações como tipo, nome do host, grupos de recursos e políticas associados e status.

Crie políticas de backup para sistemas de arquivos Unix

Antes de usar o SnapCenter para fazer backup de sistemas de arquivos Unix, você deve criar uma política de backup para o recurso ou grupo de recursos do qual deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e mantém backups. Você também pode especificar as configurações de replicação, script e tipo de backup. Criar uma política economiza tempo quando você deseja reutilizá-la em outro recurso ou grupo de recursos.

Antes de começar

- Você deve ter se preparado para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, descobrir os sistemas de arquivos e criar conexões do sistema de armazenamento.
- Se você estiver replicando Snapshots para um espelho ou armazenamento secundário de cofre, o administrador do SnapCenter deverá ter atribuído as SVMs a você para os volumes de origem e destino.
- Revise os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror . Para obter informações, consulte "Limites de objetos para sincronização ativa do SnapMirror" .

Sobre esta tarefa

- SnapLock
  - Se a opção 'Manter as cópias de backup por um número específico de dias' for selecionada, o período de retenção do SnapLock deverá ser menor ou igual aos dias de retenção mencionados.

    Especificar um período de bloqueio de Snapshot impede a exclusão dos Snapshots até que o período de retenção expire. Isso pode levar à retenção de um número maior de Snapshots do que a contagem especificada na política.

  Para o ONTAP 9.12.1 e versões anteriores, os clones criados a partir dos SnapLock Vault Snapshots como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Selecione **Sistemas de arquivos Unix** na lista suspensa.
4. Clique em **Novo**.

5. Na página Nome, insira o nome e os detalhes da política.
6. Na página Backup e Replicação, execute as seguintes ações:

   a. Especifique as configurações de backup.
   b. Especifique a frequência da programação selecionando **Sob demanda**, **Por hora**, **Diariamente**, **Semanalmente** ou **Mensalmente**.
   c. Na seção Selecionar opções de replicação secundária, selecione uma ou ambas as seguintes opções de replicação secundária:

Para este campo…	**Faça isso…**
Atualizar o SnapMirror após criar uma cópia local do Snapshot	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Esta opção deve ser habilitada para sincronização ativa do SnapMirror .
Atualizar o SnapVault após criar uma cópia local do Snapshot	Selecione esta opção para executar a replicação de backup de disco para disco (backups do SnapVault).
Contagem de novas tentativas de erro	Insira o número máximo de tentativas de replicação que podem ser permitidas antes que a operação seja interrompida.

7. Na página Retenção, especifique as configurações de retenção para o tipo de backup e o tipo de agendamento selecionado na página Backup e Replicação:

Se você quiser…	Então…

Mantenha um certo número de Snapshots	Selecione **Cópias a serem mantidas** e especifique o número de Snapshots que você deseja manter. Se o número de Snapshots exceder o número especificado, os Snapshots serão excluídos, com as cópias mais antigas sendo excluídas primeiro. O valor máximo de retenção é 1018. Os backups falharão se a retenção for definida como um valor maior do que o suportado pela versão subjacente do ONTAP . Você deve definir a contagem de retenção como 2 ou mais se planeja habilitar a replicação do SnapVault . Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro Snapshot será o Snapshot de referência para o relacionamento SnapVault até que um Snapshot mais recente seja replicado para o destino.
Mantenha os Snapshots por um certo número de dias	Selecione **Manter cópias por** e especifique o número de dias pelos quais você deseja manter os Snapshots antes de excluí-los.
Período de bloqueio de cópia de instantâneo	Selecione **Período de bloqueio de cópia de instantâneo** e especifique a duração em dias, meses ou anos. O período de retenção do Snaplock deve ser inferior a 100 anos.

8. Selecione o rótulo da política.

Você pode atribuir rótulos SnapMirror a snapshots primários para replicação remota, permitindo que os snapshots primários descarreguem a operação de replicação de snapshots do SnapCenter para sistemas secundários ONTAP . Isso pode ser feito sem habilitar a opção SnapMirror ou SnapVault na página de política.

9. Na página Script, insira o caminho e os argumentos do prescript ou postscript que você deseja executar antes ou depois da operação de backup, respectivamente.

Você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in no caminho _ /opt/ NetApp/snapcenter/scc/etc/allowed_commands.config_.

Você também pode especificar o valor do tempo limite do script. O valor padrão é 60 segundos.

10. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas para sistemas de arquivos Unix

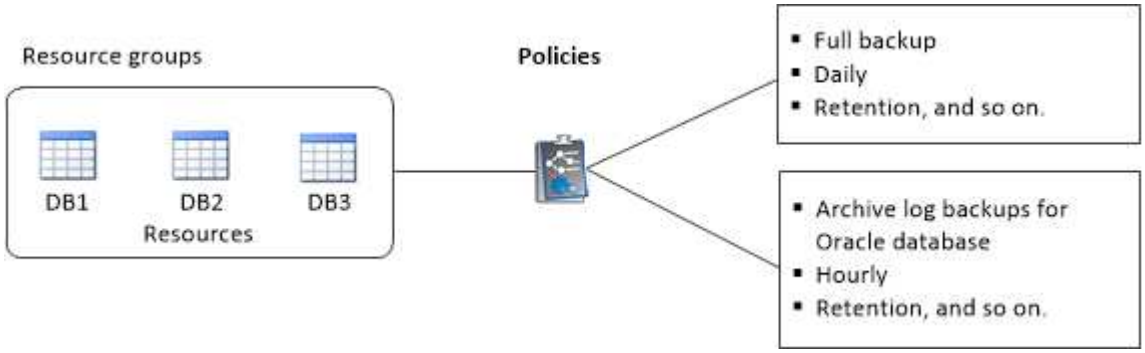
Um grupo de recursos é um contêiner onde você adiciona recursos que deseja fazer backup e proteger. Um grupo de recursos permite que você faça backup de todos os dados associados aos sistemas de arquivos.

Sobre esta tarefa

- Um banco de dados com arquivos em grupos de discos ASM deve estar no estado "MONT" ou "OPEN" para verificar seus backups usando o utilitário Oracle DBVERIFY.

  Anexe uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que você deseja executar.

  A imagem a seguir ilustra o relacionamento entre recursos, grupos de recursos e políticas para bancos de dados:



- Para políticas habilitadas para SnapLock , para ONTAP 9.12.1 e versões anteriores, se você especificar um período de bloqueio de Snapshot, os clones criados a partir de Snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock . O administrador de armazenamento deve limpar manualmente os clones após o tempo de expiração do SnapLock .
- Não há suporte para adicionar novos sistemas de arquivos sem sincronização ativa do SnapMirror a um grupo de recursos existente que contém recursos com sincronização ativa do SnapMirror .
- Não há suporte para adicionar novos sistemas de arquivos a um grupo de recursos existente no modo de failover da sincronização ativa do SnapMirror . Você pode adicionar recursos ao grupo de recursos somente no estado regular ou de failback.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:
   a. Insira um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 caracteres.

   b. Insira um ou mais rótulos no campo Tag para ajudar você a pesquisar o grupo de recursos posteriormente.

      Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar

posteriormente todos os grupos de recursos associados à tag RH.

c. Marque a caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

   Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

4. Na página Recursos, selecione um nome de host de sistemas de arquivos Unix na lista suspensa **Host**.

   Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos da seção Recursos Disponíveis e mova-os para a seção Recursos Selecionados.
6. Na página Configurações do aplicativo, faça o seguinte:
   - Selecione a seta Scripts e insira os comandos pre e post para operações de inatividade, instantâneo e ativação/desativação. Você também pode inserir os pré-comandos a serem executados antes de sair em caso de falha.
   - Selecione uma das opções de consistência de backup:
     - Selecione **Consistência do sistema de arquivos** se quiser garantir que os dados armazenados em cache do sistema de arquivos sejam liberados antes de criar o backup e que nenhuma operação de entrada ou saída seja permitida no sistema de arquivos durante a criação do backup.

       Para consistência do sistema de arquivos, serão tirados instantâneos do grupo de consistência para LUNs envolvidos no grupo de volumes.

     - Selecione **Crash Consistent** se quiser garantir que os dados armazenados em cache do sistema de arquivos sejam limpos antes de criar o backup.

       Se você tiver adicionado diferentes sistemas de arquivos no grupo de recursos, todos os volumes de diferentes sistemas de arquivos no grupo de recursos serão colocados em um grupo de Consistência.

7. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em + .

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

   c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

      Onde *policy_name* é o nome da política que você selecionou.

Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

   Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

9. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e habilite proteção secundária para sistemas de arquivos Unix em sistemas ASA r2

Você deve criar o grupo de recursos para adicionar os recursos que estão nos sistemas ASA r2. Você também pode provisionar a proteção secundária ao criar o grupo de recursos.

Antes de começar

- Você deve garantir que não está adicionando recursos do ONTAP 9.x e recursos do ASA r2 ao mesmo grupo de recursos.
- Você deve garantir que não tenha um banco de dados com recursos ONTAP 9.x e recursos ASA r2.

Sobre esta tarefa

- A proteção secundária estará disponível somente se o usuário conectado estiver atribuído à função que tem o recurso **SecondaryProtection** habilitado.
- Se você habilitar a proteção secundária, o grupo de recursos será colocado no modo de manutenção durante a criação dos grupos de consistência primário e secundário. Depois que os grupos de consistência primário e secundário são criados, o grupo de recursos é retirado do modo de manutenção.
- O SnapCenter não oferece suporte à proteção secundária para um recurso clone.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:
   a. Insira um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 caracteres.

   b. Insira um ou mais rótulos no campo Tag para ajudar você a pesquisar o grupo de recursos posteriormente.

      Por exemplo, se você adicionar RH como uma tag a vários grupos de recursos, poderá encontrar

posteriormente todos os grupos de recursos associados à tag RH.

c. Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

   Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um registro de data e hora é anexado ao nome do Snapshot.

d. Especifique os destinos dos arquivos de log de arquivamento dos quais você não deseja fazer backup.

   Você deve usar exatamente o mesmo destino definido no aplicativo, incluindo o prefixo, se necessário.

4. Na página Recursos, selecione o nome do host do banco de dados na lista suspensa **Host**.

   Os recursos são listados na seção Recursos Disponíveis somente se o recurso for descoberto com sucesso. Se você adicionou recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois que você atualizar sua lista de recursos.

5. Selecione os recursos do ASA r2 na seção Recursos disponíveis e mova-os para a seção Recursos selecionados.
6. Na página Configurações do aplicativo, selecione a opção de backup.
7. Na página Políticas, execute as seguintes etapas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você também pode criar uma política clicando em + .

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique + na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.

   c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

      Onde *policy_name* é o nome da política que você selecionou.

      Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

   Os agendamentos de backup de terceiros não são suportados quando se sobrepõem aos agendamentos de backup do SnapCenter .

8. Se a proteção secundária estiver habilitada para a política selecionada, a página Proteção Secundária será exibida e você precisará executar as seguintes etapas:

   a. Selecione o tipo de política de replicação.

      A política de replicação síncrona não é suportada.

b. Especifique o sufixo do grupo de consistência que você deseja usar.

c. Nos menus suspensos Cluster de destino e SVM de destino, selecione o cluster emparelhado e o SVM que você deseja usar.

> O cluster e o peering de SVM não são suportados pelo SnapCenter. Você deve usar o System Manager ou as CLIs do ONTAP para executar o peering de cluster e SVM.

> Se os recursos já estiverem protegidos fora do SnapCenter, eles serão exibidos na seção Recursos Protegidos Secundários.

1. Na página Verificação, execute as seguintes etapas:

   a. Clique em **Carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para realizar a verificação no armazenamento secundário.

   b. Clique + na coluna Configurar agendamentos para configurar o agendamento de verificação para todos os tipos de agendamento da política.

   c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name, execute as seguintes ações:

Se você quiser…	Faça isso…
Executar verificação após o backup	Selecione **Executar verificação após backup**.
Agendar uma verificação	Selecione **Executar verificação agendada** e depois selecione o tipo de agendamento na lista suspensa.

   d. Selecione **Verificar no local secundário** para verificar seus backups no sistema de armazenamento secundário.

   e. Clique em **OK**.

   Os agendamentos de verificação configurados são listados na coluna Agendamentos Aplicados.

2. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação realizada no grupo de recursos, selecione **Anexar relatório de trabalho**.

   > Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

3. Revise o resumo e clique em **Concluir**.

Fazer backup de sistemas de arquivos Unix

Se um recurso não fizer parte de nenhum grupo de recursos, você poderá fazer backup do recurso na página Recursos.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, selecione **Caminho** na lista Exibir.
3. Clique e, em seguida, selecione o nome do host e os sistemas de arquivos Unix para filtrar os recursos.
4. Selecione o sistema de arquivos do qual você deseja fazer backup.
5. Na página Recursos, você pode executar as seguintes etapas:
   a. Marque a caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

      Por exemplo, `customtext_policy_hostname` ou `resource_hostname` . Um registro de data e hora é anexado ao nome do Snapshot por padrão.

6. Na página Configurações do aplicativo, faça o seguinte:
   - Selecione a seta Scripts e insira os comandos pre e post para operações de inatividade, instantâneo e ativação/desativação. Você também pode inserir os pré-comandos a serem executados antes de sair em caso de falha.
   - Selecione uma das opções de consistência de backup:
     - Selecione **Consistência do sistema de arquivos** se quiser garantir que os dados armazenados em cache do sistema de arquivos sejam liberados antes de criar o backup e que nenhuma operação seja executada no sistema de arquivos durante a criação do backup.
     - Selecione **Crash Consistent** se quiser garantir que os dados armazenados em cache do sistema de arquivos sejam limpos antes de criar o backup.
7. Na página Políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.

      Você pode criar uma política clicando em .

      Na seção Configurar agendamentos para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique na coluna Configurar agendamentos para configurar um agendamento para a política desejada.
   c. Na janela Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione `OK` .

      policy_name é o nome da política que você selecionou.

   Os agendamentos configurados são listados na coluna Agendamentos Aplicados.

8. Na página Notificação, selecione os cenários nos quais você deseja enviar os e-mails na lista suspensa **Preferência de e-mail**.

   Você deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação de backup realizada no recurso, selecione **Anexar relatório de tarefa**.

Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando PowerShell `Set-SmSmtpServer` .

9. Revise o resumo e clique em **Concluir**.

   A página de topologia é exibida.

10. Clique em **Fazer backup agora**.
11. Na página Backup, execute as seguintes etapas:
    a. Se você aplicou várias políticas ao recurso, na lista suspensa Política, selecione a política que deseja usar para backup.

       Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

    b. Clique em **Backup**.
12. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Fazer backup de grupos de recursos de sistemas de arquivos Unix

Você pode fazer backup dos sistemas de arquivos Unix definidos no grupo de recursos. Você pode fazer backup de um grupo de recursos sob demanda na página Recursos. Se um grupo de recursos tiver uma política anexada e um agendamento configurado, os backups serão criados de acordo com o agendamento.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.
3. Digite o nome do grupo de recursos na caixa de pesquisa ou clique em e selecione a tag.

   Clique para fechar o painel de filtro.

4. Na página Grupo de recursos, selecione o grupo de recursos para fazer backup.
5. Na página Backup, execute as seguintes etapas:
    a. Se você tiver várias políticas associadas ao grupo de recursos, selecione a política de backup que deseja usar na lista suspensa **Política**.

       Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

    b. Selecione **Backup**.
6. Monitore o progresso selecionando **Monitorar > Trabalhos**.

Monitorar backup de sistemas de arquivos Unix

Aprenda a monitorar o progresso das operações de backup e proteção de dados.

Monitorar operações de backup de sistemas de arquivos Unix

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Talvez você queira verificar o progresso para determinar quando ele foi concluído ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado correspondente das operações:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **Trabalhos**.
3. Na página Trabalhos, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de backup sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Backup**.
   d. No menu suspenso **Status**, selecione o status do backup.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione uma tarefa de backup e clique em **Detalhes** para visualizar os detalhes da tarefa.

   Embora o status do trabalho de backup seja exibido , ao clicar em detalhes do trabalho, você poderá ver que algumas das tarefas filhas da operação de backup ainda estão em andamento ou marcadas com sinais de alerta.

5. Na página Detalhes do trabalho, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Monitore as operações de proteção de dados no painel Atividade

O painel Atividade exibe as cinco operações mais recentes realizadas. O painel Atividade também exibe quando a operação foi iniciada e o status da operação.

O painel Atividade exibe informações sobre operações de backup, restauração, clonagem e backup agendado.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Clique no painel Atividade para visualizar as cinco operações mais recentes.

Quando você clica em uma das operações, os detalhes da operação são listados na página **Detalhes do trabalho**.

Exibir sistemas de arquivos Unix protegidos na página Topologia

Ao se preparar para fazer backup, restaurar ou clonar um recurso, pode ser útil visualizar uma representação gráfica de todos os backups, sistemas de arquivos restaurados e clones no armazenamento primário e secundário.

Sobre esta tarefa

Na página Topologia, você pode ver todos os backups, sistemas de arquivos restaurados e clones disponíveis para o recurso ou grupo de recursos selecionado. Você pode visualizar os detalhes desses backups, sistemas de arquivos restaurados e clones e selecioná-los para executar operações de proteção de dados.

Você pode revisar os seguintes ícones na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no armazenamento primário ou secundário (cópias espelhadas ou cópias do Vault).

-  exibe o número de backups e clones que estão disponíveis no armazenamento primário.
-  exibe o número de backups e clones que são espelhados no armazenamento secundário usando a tecnologia SnapMirror .
-  exibe o número de backups e clones que são replicados no armazenamento secundário usando a tecnologia SnapVault .

  O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou 6 backups usando uma política para manter apenas 4 backups, o número de backups exibidos será 6.

Clones de um backup de um espelho flexível em termos de versão em um volume do tipo mirror-vault são exibidos na exibição de topologia, mas a contagem de backups de espelho na exibição de topologia não inclui o backup flexível em termos de versão.

Se você tiver um relacionamento secundário como sincronização ativa do SnapMirror (inicialmente lançado como SnapMirror Business Continuity [SM-BC]), poderá ver os seguintes ícones adicionais:

-  O site de réplica está no ar.
-  O site de réplicas está fora do ar.
-  O espelho secundário ou o relacionamento do cofre não foram restabelecidos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso na exibição de detalhes do recurso ou na exibição de detalhes do grupo de recursos.

   Se o recurso estiver protegido, a página Topologia do recurso selecionado será exibida.

4. Revise o cartão Resumo para ver um resumo do número de backups e clones disponíveis no armazenamento primário e secundário.

   A seção Cartão de Resumo exibe o número total de backups e clones.

   Clicar no botão **Atualizar** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clicar no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Uma programação semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o sistema de arquivos estiver distribuído em vários volumes, o tempo de expiração do SnapLock para o backup será o maior tempo de expiração do SnapLock definido para um Snapshot em um volume. O maior tempo de expiração do SnapLock é recuperado do ONTAP.

   Para sincronização ativa do SnapMirror , clicar no botão **Atualizar** atualiza o inventário de backup do SnapCenter consultando o ONTAP para sites primários e de réplica. Uma programação semanal também executa essa atividade para todos os bancos de dados que contêm o relacionamento de sincronização ativo do SnapMirror .

   - Para sincronização ativa do SnapMirror e somente para o ONTAP 9.14.1, os relacionamentos Async Mirror ou Async MirrorVault com o novo destino primário devem ser configurados manualmente após o failover. A partir do ONTAP 9.15.1, o Async Mirror ou o Async MirrorVault são configurados automaticamente para o novo destino principal.
   - Após o failover, um backup deve ser criado para que o SnapCenter esteja ciente do failover. Você pode clicar em **Atualizar** somente após um backup ter sido criado.
5. Na exibição Gerenciar cópias, clique em **Backups** ou **Clones** do armazenamento primário ou secundário para ver detalhes de um backup ou clone.

   Os detalhes dos backups e clones são exibidos em formato de tabela.

6. Selecione o backup na tabela e clique nos ícones de proteção de dados para executar operações de restauração, clonagem e exclusão.

   Não é possível renomear ou excluir backups que estejam no armazenamento secundário.

7. Se você quiser excluir um clone, selecione o clone na tabela e clique em .

Exemplo mostrando backups e clones no armazenamento primário

Restaurar e recuperar sistemas de arquivos Unix

Restaurar sistemas de arquivos Unix

Em caso de perda de dados, você pode usar o SnapCenter para restaurar sistemas de arquivos Unix.

Sobre esta tarefa

- Você deve executar os seguintes comandos para estabelecer a conexão com o SnapCenter Server, listar os backups, recuperar suas informações e restaurar o backup.

  As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando Get-Help *command_name*. Alternativamente, você também pode consultar o "Guia de referência de comandos do software SnapCenter" .

- Para a operação de restauração de sincronização ativa do SnapMirror , você deve selecionar o backup do local principal.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Caminho** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o sistema de arquivos na exibição de detalhes ou na exibição de detalhes do grupo de recursos.

A página de topologia é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
5. Selecione o backup da tabela e clique em *  *.
6. Na página Escopo de restauração:
   - Para sistemas de arquivos NFS, por padrão, a restauração **Conectar e Copiar** é selecionada. Você também pode selecionar **Reverter Volume** ou **Restauração Rápida**.
   - Para sistemas de arquivos não NFS, o escopo de restauração é selecionado dependendo do layout.

     Os novos arquivos criados após o backup podem não estar disponíveis após a restauração, dependendo do tipo e do layout do sistema de arquivos.
7. Na página PreOps, insira comandos de pré-restauração a serem executados antes de executar um trabalho de restauração.
8. Na página PostOps, insira comandos de pós-restauração a serem executados após a execução de um trabalho de restauração.

   Você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in no local */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config* path.
9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar as notificações por e-mail.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação de restauração realizada, selecione **Anexar relatório de tarefa**.

   Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.
10. Revise o resumo e clique em **Concluir**.

    Se a operação de restauração falhar, a reversão não será suportada.

    Em caso de restauração de um sistema de arquivos residente em um grupo de volumes, o conteúdo antigo no sistema de arquivos não é excluído. Somente o conteúdo do sistema de arquivos clonado será copiado para o sistema de arquivos de origem. Isso é aplicável quando há vários sistemas de arquivos no grupo de volumes e restaurações do sistema de arquivos NFS padrão.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Monitorar operações de restauração de sistemas de arquivos Unix

Você pode monitorar o progresso de diferentes operações de restauração do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os estados pós-restauração descrevem as condições do recurso após uma operação de restauração e quaisquer outras ações de restauração que você possa tomar.

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente as operações de restauração sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Restaurar**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Aplicar** para visualizar as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

   O botão **Exibir logs** exibe os logs detalhados da operação selecionada.

Clonar sistemas de arquivos Unix

Clonar backup do sistema de arquivos Unix

Você pode usar o SnapCenter para clonar o sistema de arquivos Unix usando o backup do sistema de arquivos.

Antes de começar

- Você pode pular a atualização do arquivo fstab definindo o valor de *SKIP_FSTAB_UPDATE* como **true** no arquivo *agent.properties* localizado em */opt/ NetApp/snapcenter/scc/etc*.
- Você pode ter um nome de volume clone estático e um caminho de junção definindo o valor de *USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT* como **true** no arquivo *agent.properties* localizado em */opt/ NetApp/snapcenter/scc/etc*. Após atualizar o arquivo, você deve reiniciar o serviço do criador do plug-in SnapCenter executando o comando: `/opt/NetApp/snapcenter/scc/bin/scc restart` .

  Exemplo: Sem essa propriedade, o nome do volume clone e o caminho da junção serão como <Source_volume_name>_Clone_<Timestamp>, mas agora serão

<Source_volume_name>_Clone_<Clone_Name>

Isso mantém o nome constante para que você possa manter o arquivo fstab atualizado manualmente, caso não prefira atualizar o fstab pelo SnapCenter.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Caminho** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o sistema de arquivos na exibição de detalhes ou na exibição de detalhes do grupo de recursos.

   A página de topologia é exibida.

4. Na exibição Gerenciar cópias, selecione os backups entre Cópias locais (primárias), Cópias espelhadas (secundárias) ou Cópias de cofre (secundárias).
5. Selecione o backup da tabela e clique em *  *.
6. Na página Localização, execute as seguintes ações:

Para este campo…	Faça isso…
Servidor clone	Por padrão, o host de origem é preenchido.
Ponto de montagem do clone	Especifique o caminho onde o sistema de arquivos será montado.

7. Na página Scripts, execute as seguintes etapas:
   a. Insira os comandos para pré-clonagem ou pós-clonagem que devem ser executados antes ou depois da operação de clonagem, respectivamente.

   Você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in no caminho */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*.

8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-mail. Se você quiser anexar o relatório da operação de clonagem realizada, selecione **Anexar relatório de trabalho**.

   Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando a GUI ou o comando Set-SmSmtpServer do PowerShell.

9. Revise o resumo e clique em **Concluir**.
10. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Dividir um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido se torna independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clone em um clone intermediário.

  Por exemplo, depois de criar o clone1 a partir de um backup de banco de dados, você pode criar um backup do clone1 e então clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e você não pode executar a operação de divisão de clone no clone1. No entanto, você pode executar a operação de divisão de clone no clone2.

  Após dividir o clone2, você pode executar a operação de divisão do clone no clone1 porque o clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e os trabalhos de clonagem do clone são excluídos.
- Para obter informações sobre as operações de divisão de volume do FlexClone , consulte "Dividir um volume FlexClone de seu volume pai" .
- Certifique-se de que o volume ou agregado no sistema de armazenamento esteja online.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página **Recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicações de banco de dados	Selecione **Banco de dados** na lista Exibir.
Para sistemas de arquivos	Selecione **Caminho** na lista Exibir.

3. Selecione o recurso apropriado na lista.

   A página de topologia de recursos é exibida.

4. Na exibição **Gerenciar cópias**, selecione o recurso clonado (por exemplo, o banco de dados ou LUN) e clique em *  *.
5. Revise o tamanho estimado do clone que será dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

   A operação de divisão do clone para de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clone e, em seguida, tentar novamente a operação de divisão de clone.

   Se você quiser um tempo de pesquisa maior ou menor para verificar se o clone está dividido ou não, você pode alterar o valor do parâmetro *CloneSplitStatusCheckPollTime* no arquivo *SMCoreServiceHost.exe.config* para definir o intervalo de tempo para o SMCore pesquisar o status da operação de divisão do clone. O valor está em milissegundos e o valor padrão é 5 minutos.

   Por exemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

A operação de início da divisão do clone falha se um backup, uma restauração ou outra divisão do clone estiver em andamento. Você deve reiniciar a operação de divisão do clone somente após a conclusão das operações em execução.

Informações relacionadas

"O clone ou a verificação do SnapCenter falham com o agregado inexistente"

Monitorar operações de clonagem de sistemas de arquivos Unix

Você pode monitorar o progresso das operações de clonagem do SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento de uma operação para determinar quando ela foi concluída ou se há algum problema.

Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Jobs**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que somente operações de clonagem sejam listadas.
   b. Especifique as datas de início e término.
   c. Na lista suspensa **Tipo**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Aplicar** para visualizar as operações concluídas com sucesso.
4. Selecione o trabalho de clonagem e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página Detalhes do trabalho, clique em **Exibir registros**.

Proteja aplicativos em execução no Azure NetApp Files

Proteja aplicativos em execução no Azure NetApp Files

O SnapCenter oferece suporte à proteção de seus aplicativos, como Oracle, SQL e SAP HANA, que residem no Azure NetApp Files. A partir da versão 6.0.1, o SnapCenter oferece suporte ao recurso de backup do Azure NetApp Files , que expande os recursos de proteção de dados do Azure NetApp Files ao fornecer uma solução de backup totalmente gerenciada para recuperação, arquivamento e conformidade de longo prazo.

O Azure NetApp Files é uma solução de armazenamento premium que pode ser cara para retenção de backup de longo prazo. Para otimizar custos, você pode mover os backups do armazenamento do Azure NetApp Files para um armazenamento de objetos do Azure. A partir do SnapCenter 6.0.1, você pode fazer backup e clonar aplicativos que residem no Azure NetApp Files para o Azure Blob Storage (armazenamento de objetos). Você pode manter duas cópias dos seus dados, cópias de instantâneos de volume no armazenamento do Azure NetApp Files para recuperação de curto prazo e outra cópia no Armazenamento de Blobs do Azure para recuperação de longo prazo.

Quando uma política com backup do Azure NetApp Files é habilitada e associada a um recurso, o SnapCenter lida com a criação de instantâneos de volume e o backup deles no Armazenamento de Blobs do Azure. O SnapCenter cria o Backup Vault e habilita o backup para o volume. Se você tiver habilitado o backup para o volume, o SnapCenter utilizará o cofre existente.

Limitações

- As funcionalidades de armazenamento de objetos para sistemas de armazenamento FAS, ASA ou AFF ONTAP e Amazon FSx for NetApp ONTAP não são suportadas.
- Os fluxos de trabalho de montagem e catálogo do Oracle e SAP HANA não são suportados para backups de armazenamento de objetos, mas são suportados para snapshots.
- Os clones do Oracle PDB não são suportados para backups de armazenamento de objetos, mas são suportados para snapshots.
- A verificação de backup do armazenamento de objetos, o suporte à API REST, o gerenciamento do ciclo de vida do clone do armazenamento de objetos e os recursos de relatório para backups de armazenamento de objetos não são suportados.
- Não há suporte para restauração de backups no Armazenamento de Blobs do Azure para o Azure NetApp Files . Você pode usar a opção clone como alternativa.
- A divisão de clones não é suportada.

Instale o SnapCenter e crie credenciais

Instalar o SnapCenter na Máquina Virtual do Azure

Você pode baixar o SnapCenter software no site de suporte da NetApp e instalar o software na máquina virtual do Azure.

Antes de começar

- Certifique-se de que a máquina virtual do Azure Windows atenda aos requisitos para instalação do SnapCenter Server. Para obter informações, consulte"Requisitos para instalar o SnapCenter Server" .
- Se você é novo no Azure NetApp Files e não tem uma conta NetApp existente, certifique-se de ter se registrado para poder acessar o SnapCenter Software. Para obter informações, consulte"Registre-se para acessar o SnapCenter software" .

Passos

1. Baixe o pacote de instalação do SnapCenter Server em "Site de suporte da NetApp" .
2. Inicie a instalação do SnapCenter Server clicando duas vezes no arquivo .exe baixado.

   Após iniciar a instalação, todas as pré-verificações são realizadas e, se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas são exibidas. Você pode ignorar as mensagens de aviso e prosseguir com a instalação; no entanto, os erros deverão ser corrigidos.

3. Revise os valores pré-preenchidos necessários para a instalação do SnapCenter Server e modifique-os, se necessário.

   Você não precisa especificar a senha para o banco de dados do repositório do MySQL Server. Durante a instalação do SnapCenter Server, a senha é gerada automaticamente.

   O caractere especial “%” não é suportado no caminho personalizado para o banco de dados do repositório. Se você incluir “%” no caminho, a instalação falhará.

4. Clique em **Instalar agora**.

   Se você tiver especificado algum valor inválido, mensagens de erro apropriadas serão exibidas. Você deve inserir os valores novamente e então iniciar a instalação.

   Se você clicar no botão **Cancelar**, a etapa que está sendo executada será concluída e, em seguida, iniciará a operação de reversão. O SnapCenter Server será completamente removido do host.

   Entretanto, se você clicar em **Cancelar** quando as operações "Reinicialização do site do SnapCenter Server" ou "Aguardando o início do SnapCenter Server" estiverem sendo executadas, a instalação prosseguirá sem cancelar a operação.

Registre o produto para habilitar o suporte

Se você é novo na NetApp e não tem uma conta NetApp existente, registre o produto para habilitar o suporte.

Passos

1. Após instalar o SnapCenter, navegue até **Ajuda > Sobre**.
2. Na caixa de diálogo *Sobre o SnapCenter*, anote a instância do SnapCenter , um número de 20 dígitos que começa com 971.
3. Clique https://register.netapp.com .
4. Clique em *Não sou um cliente registrado da NetApp *.
5. Especifique seus dados para se registrar.
6. Deixe o campo SN de referência da NetApp em branco.
7. Selecione * SnapCenter* no menu suspenso Linha de produtos.

8. Selecione o provedor de cobrança.
9. Insira o ID da instância do SnapCenter de 20 dígitos.
10. Clique em **Enviar**.

Crie a credencial do Azure no SnapCenter

Você deve criar a credencial do Azure no SnapCenter para acessar a conta do Azure NetApp .

Antes de começar

- Certifique-se de ter criado a entidade de serviço no Azure.
- Certifique-se de ter o ID do locatário, o ID do cliente e a chave secreta associados à entidade de serviço disponíveis.
  - O ID do locatário pode ser encontrado no Portal do Azure, na página Visão geral do ID de entrada.
  - O ID do cliente também é conhecido como ID do aplicativo para o aplicativo/serviço principal corporativo. Isso pode ser encontrado no Portal do Azure, na página Visão geral do aplicativo empresarial que você criou para atuar como a entidade de serviço do SnapCenter.
  - A Chave Secreta do Cliente também é conhecida como Valor Secreto. Você pode criar esse segredo do cliente no Portal do Azure navegando até **Registros de aplicativo** em ID de entrada. Depois de selecionar o aplicativo corporativo que você criou, navegue até **Certificados e segredos** e depois **Novo segredo do cliente**.

    O valor secreto só pode ser acessado quando criado. Você não poderá acessá-lo mais tarde.

  - O Principal de Serviço precisa receber permissões. A função de Colaborador permitirá que a entidade de serviço execute as ações necessárias no Azure. Isso pode ser concedido na página Controle de Acesso (IAM) na página Assinatura.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.
4. Na página Credencial, especifique as seguintes informações necessárias para criar a credencial.

Para este campo…	Faça isso…
Nome da credencial	Digite um nome para a credencial.
Modo de autenticação	Selecione **Credencial do Azure** na lista suspensa.
ID do inquilino	Digite o ID do inquilino.
ID do cliente	Digite o ID do cliente.
Chave secreta do cliente	Digite a chave secreta do cliente.

5. Clique em **OK**.

Configurar a conta de armazenamento do Azure

Você deve configurar a conta de armazenamento do Azure no SnapCenter.

A conta de armazenamento do Azure contém detalhes sobre o ID da assinatura, a credencial do Azure e a conta do Azure NetApp .

As licenças padrão e baseadas em capacidade não são necessárias para o Azure NetApp Files.

Passos

1. No painel de navegação esquerdo, clique em **Sistemas de armazenamento**.
2. Na página Sistemas de Armazenamento, selecione * Azure NetApp Files* e clique em **Novo**.
3. Selecione a credencial, o ID da assinatura e a conta NetApp nas respectivas listas suspensas.
4. Clique em **Enviar**.

Crie a credencial para adicionar o host do plug-in

O SnapCenter usa credenciais para autenticar usuários para operações do SnapCenter .

Você deve criar credenciais para instalar plug-ins do SnapCenter e credenciais adicionais para executar operações de proteção de dados.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credencial**.
3. Clique em **Novo**.
4. Na página Credencial, especifique as seguintes informações necessárias para criar a credencial.

Para este campo…	Faça isso…
Nome da credencial	Digite um nome para a credencial.
Modo de autenticação	Selecione o modo de autenticação na lista suspensa.
Tipo de autenticação	Selecione **Baseado em senha** ou **Baseado em chave SSH** (somente para host Linux).
Nome de usuário	Especifique o nome de usuário.
Senha	Se você selecionou Autenticação baseada em senha, especifique a senha.

Para este campo…	Faça isso…
Chave privada SSH	Se você selecionou a autenticação baseada em chave SSH, especifique a chave privada.
Use privilégios sudo	Marque a caixa de seleção Usar privilégios sudo se estiver criando credenciais para um usuário não root. Isso é aplicável somente para usuários do Linux.

5. Clique em **OK**.

Proteja bancos de dados SAP HANA

Adicionar hosts e instalar o plug-in SnapCenter para o banco de dados SAP HANA

Você deve usar a página Adicionar Host do SnapCenter para adicionar hosts e, em seguida, instalar os pacotes de plug-ins. Os plug-ins são instalados automaticamente nos hosts remotos.

Antes de começar

- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.
- Se você estiver instalando no host centralizado, certifique-se de que o software cliente SAP HANA esteja instalado nesse host e abra as portas necessárias no host do banco de dados SAP HANA para executar as consultas SQL do HDB remotamente.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se a guia **Hosts gerenciados** está selecionada.
3. Clique em **Adicionar**.
4. Na página Hosts, execute as seguintes ações:
   a. No campo Tipo de host, selecione o tipo de host.
   b. No campo Nome do host, insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host.
   c. No campo Credenciais, insira a credencial que você criou.
5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a serem instalados.
6. (Opcional) Clique em **Mais opções** e especifique os detalhes.
7. Clique em **Enviar**.
8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirmar e Enviar**.

Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós do cluster.

9. Monitore o progresso da instalação.

Adicionar banco de dados SAP HANA

Você deve adicionar o banco de dados SAP HANA manualmente.

Sobre esta tarefa

Os recursos precisam ser adicionados manualmente se o plug-in estiver instalado em um servidor centralizado. Se o plug-in SAP HANA estiver instalado no host do banco de dados HANA, o sistema HANA será descoberto automaticamente.

A descoberta automática não é suportada para configuração de vários hosts do HANA; eles devem ser adicionados somente por meio de plug-in centralizado.

Passos

1. No painel de navegação esquerdo, selecione o plug-in SnapCenter para banco de dados SAP HANA na lista suspensa e clique em **Recursos**.
2. Na página Recursos, clique em **Adicionar banco de dados SAP HANA**.
3. Na página Fornecer detalhes do recurso, execute as seguintes ações:
   a. Insira o tipo de recurso como Contêiner Único, Contêiner de Banco de Dados Multilocatário ou Volume sem dados.
   b. Digite o nome do sistema SAP HANA.
   c. Digite o ID do sistema (SID).
   d. Selecione o host do plug-in.
   e. Insira a chave para conectar ao sistema SAP HANA.
   f. Digite o nome de usuário para o qual a chave de armazenamento de usuário seguro do HDB está configurada.
4. Na página Fornecer espaço de armazenamento, selecione * Azure NetApp Files* como o tipo de armazenamento.
   a. Selecione a conta do Azure NetApp .
   b. Selecione o pool de capacidade e os volumes associados.
   c. Clique em **Salvar**.
5. Revise o resumo e clique em **Concluir**.

Crie políticas de backup para bancos de dados SAP HANA

Antes de usar o SnapCenter para fazer backup de recursos do banco de dados SAP HANA, você deve criar uma política de backup para o recurso ou grupo de recursos que deseja fazer backup.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.

3. Clique em **Novo**.
4. Na página Nome, insira o nome e a descrição da política.
5. Na página Tipo de política, execute as seguintes etapas:
   a. Selecione * Azure NetApp Files* como o tipo de armazenamento.
   b. Selecione **Baseado em arquivo** se quiser executar uma verificação de integridade do banco de dados.
   c. Selecione **Baseado em instantâneo** se quiser criar um backup usando a tecnologia Snapshot.
6. Na página Snapshot e backup, execute as seguintes etapas:
   a. Selecione a frequência do backup agendado.
   b. Especifique as configurações de retenção.
   c. Se você quiser habilitar o backup do Azure NetApp Files , selecione **Habilitar backup** e especifique as configurações de retenção.
7. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas de backup do SAP HANA

Um grupo de recursos é o contêiner ao qual você deve adicionar recursos que deseja fazer backup e proteger.

Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente. Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que deseja executar.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Insira um nome para o grupo de recursos.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos.
Use formato de nome personalizado para cópia do Snapshot	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

4. Na página Recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Tipo de recurso**.
5. Selecione os recursos na seção **Recursos disponíveis** e clique na seta para a direita para movê-los para a seção **Recursos selecionados**.
6. Na página Políticas, execute as seguintes etapas:

a. Selecione uma ou mais políticas na lista suspensa.

b. Na coluna Configurar agendamentos, clique em * + * para a política que você deseja configurar.

c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.

7. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
8. Revise o resumo e clique em **Concluir**.

Fazer backup de bancos de dados SAP HANA em execução no Azure NetApp Files

Se um recurso ainda não fizer parte de nenhum grupo de recursos, você poderá fazer backup do recurso na página Recursos.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recurso, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.
3. Selecione o recurso que você deseja fazer backup.
4. Na página Recurso, selecione **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.
5. Na página Configurações do aplicativo, faça o seguinte:
   a. Selecione a seta **Backups** para definir opções adicionais de backup.
   b. Selecione a seta **Scripts** para executar comandos pré e pós para operações de inatividade, instantâneo e ativação/desativação.
   c. Selecione a seta **Configurações personalizadas** e insira os pares de valores personalizados necessários para todos os trabalhos que usam este recurso.
   d. Selecione a **Ferramenta de cópia de instantâneo > SnapCenter sem consistência do sistema de arquivos** para criar instantâneos.

      A opção **Consistência do sistema de arquivos** é aplicável somente para aplicativos executados em hosts Windows.

6. Na página Políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Selecione * + * na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.
   c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione **OK**.

      policy_name é o nome da política que você selecionou.

7. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

   Você também deve especificar os endereços de e-mail do remetente e do destinatário, e o assunto do e-

mail. O SMTP também deve ser configurado em **Configurações** > **Configurações globais**.

8. Revise o resumo e selecione **Concluir**.
9. Selecione **Fazer backup agora**.
10. Na página Backup, execute as seguintes etapas:
    a. Se várias políticas estiverem associadas ao recurso, na lista suspensa **Política**, selecione a política que você deseja usar para backup.

       Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.
11. Selecione **Backup**.
12. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Fazer backup de grupos de recursos do SAP HANA

Um grupo de recursos é uma coleção de recursos em um host. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.
3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e selecione **Fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
    a. Se várias políticas estiverem associadas ao grupo de recursos, na lista suspensa **Política**, selecione a política que você deseja usar para backup.

       Se a política selecionada para o backup sob demanda estiver associada a um agendamento de backup, os backups sob demanda serão retidos com base nas configurações de retenção especificadas para o tipo de agendamento.

    b. Selecione **Backup**.
5. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Restaurar e recuperar bancos de dados SAP HANA

Você pode restaurar e recuperar dados dos backups.

Sobre esta tarefa

Para sistemas HANA descobertos automaticamente, se a opção **Recurso Completo** for selecionada, a restauração será realizada usando a tecnologia de restauração de instantâneo de arquivo único. Se a caixa de seleção **Restauração rápida** estiver selecionada, a tecnologia de reversão de volume será usada.

Para recursos adicionados manualmente, a tecnologia Volume Revert é sempre usada.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.
3. Selecione o recurso ou selecione um grupo de recursos e, em seguida, selecione um recurso nesse grupo.
4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primário ou secundário (espelhado ou em cofre).
5. Na tabela Backup(s) primário(s), selecione o backup que deseja restaurar e clique em *  *.
6. Na página Escopo de restauração, selecione **Recurso completo**.

   Todos os volumes de dados configurados do banco de dados SAP HANA são restaurados.

7. Para sistemas HANA descobertos automaticamente, na página Escopo de recuperação, execute as seguintes ações:
   a. Selecione **Recuperar para o estado mais recente** se quiser recuperar o mais próximo possível do momento atual.
   b. Selecione **Recuperar para um ponto no tempo** se quiser recuperar para o ponto no tempo especificado.
   c. Selecione **Recuperar para backup de dados especificado** se quiser recuperar para um backup de dados específico.
   d. Selecione **Sem recuperação** se não quiser recuperar agora.
   e. Especifique os locais de backup do log.
   f. Especifique o local do catálogo de backup.
8. Na página Pré-operações, insira os comandos pre restore e unmount para executar antes de realizar um trabalho de restauração.
9. Na página Post ops, insira os comandos mount e post restore para serem executados após realizar um trabalho de restauração.
10. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

    Você também deve especificar os endereços de e-mail do remetente e do destinatário e o assunto do e-mail. O SMTP também deve ser configurado na página **Configurações** > **Configurações globais**.

11. Revise o resumo e clique em **Concluir**.
12. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Clonar backup de banco de dados SAP HANA

Você pode usar o SnapCenter para clonar um banco de dados SAP HANA usando o backup do banco de dados. Os clones criados são clones grossos e são criados no pool de capacidade pai.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, filtre os recursos da lista suspensa **Exibir** com base no tipo de recurso.

3. Selecione o recurso ou grupo de recursos.
4. Na exibição Gerenciar cópias, selecione **Backups** do sistema de armazenamento primário.
5. Selecione o backup de dados da tabela e clique em  .
6. Na página Localização, execute as seguintes ações:
   a. Selecione o host que tem o plug-in SAP HANA instalado para gerenciar o sistema HANA clonado.

      Pode ser um host de plug-in centralizado ou um host de sistema HANA.

      Se o plug-in HANA estiver instalado em um host centralizado que gerencia bancos de dados HANA em outros hosts, ao criar ou excluir clones, o SnapCenter intencionalmente ignorará as operações do lado do host (montar ou desmontar o sistema de arquivos), pois o servidor de destino é um host centralizado. Você deve usar scripts personalizados de pré ou pós-clonagem para executar operações de montagem e desmontagem.

   a. Insira o SID do SAP HANA para clonar dos backups existentes.
   b. Insira os endereços IP ou os nomes de host nos quais os volumes clonados serão exportados.
   c. Se os volumes ANF do banco de dados SAP HANA estiverem configurados em um pool de capacidade de QOS manual, especifique o QOS para os volumes clonados.

      Se o QOS para os volumes clonados não for especificado, o QOS do volume de origem será usado. Se o pool de capacidade de QOS automático for usado, o valor de QOS especificado será ignorado.
7. Na página Scripts, execute as seguintes etapas:
   a. Insira os comandos para pré-clonagem ou pós-clonagem que devem ser executados antes ou depois da operação de clonagem, respectivamente.
   b. Digite o comando mount para montar um sistema de arquivos em um host.

      Se o sistema HANA de origem for descoberto automaticamente e o plug-in do host de destino do clone estiver instalado no host SAP HANA, o SnapCenter desmontará automaticamente os volumes de dados HANA existentes no host de destino do clone e montará os volumes de dados HANA recém-clonados.
8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
9. Revise o resumo e clique em **Concluir**.
10. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

    A divisão de clones está desabilitada para clones ANF porque o clone ANF já é um volume independente criado a partir do Snapshot selecionado.

Proteja bancos de dados do Microsoft SQL Server

Adicionar hosts e instalar o plug-in SnapCenter para banco de dados SQL Server

O SnapCenter oferece suporte à proteção de dados de instâncias SQL em compartilhamentos SMB no Azure NetApp Files. As configurações autônomas e de

grupo de disponibilidade (AG) são suportadas.

Você deve usar a página Adicionar Host do SnapCenter para adicionar hosts e, em seguida, instalar o pacote de plug-ins. Os plug-ins são instalados automaticamente nos hosts remotos.

Antes de começar

- Você deve ser um usuário atribuído a uma função que tenha permissões de instalação e desinstalação de plug-ins, como a função de administrador do SnapCenter .
- Ao instalar um plug-in em um host Windows, se você especificar uma credencial que não esteja integrada ou se o usuário pertencer a um usuário de grupo de trabalho local, será necessário desabilitar o UAC no host.

Passos

1. No painel de navegação esquerdo, selecione **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Selecione **Adicionar**.
4. Na página Hosts, faça o seguinte:
   a. No campo Tipo de host, selecione o tipo de host.
   b. No campo Nome do host, insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host.
   c. No campo Credenciais, insira a credencial que você criou.
5. Na seção **Selecionar plug-ins para instalar**, selecione os plug-ins a serem instalados.
6. (Opcional) Clique em **Mais opções** e especifique os detalhes.
7. Selecione **Enviar**.
8. Selecione **Configurar diretório de log** e na página Configurar diretório de log do host, insira o caminho SMB do diretório de log do host e clique em **Salvar**.
9. Clique em **Enviar** e monitore o progresso da instalação.

Crie políticas de backup para bancos de dados SQL Server

Você pode criar uma política de backup para o recurso ou grupo de recursos antes de usar o SnapCenter para fazer backup de recursos do SQL Server ou pode criar uma política de backup no momento em que cria um grupo de recursos ou faz backup de um único recurso.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Clique em **Novo**.
4. Na página Nome, insira o nome e a descrição da política.
5. Na página Tipo de política, execute as seguintes etapas:
   a. Selecione * Azure NetApp Files* como o tipo de armazenamento.
   b. Selecione o tipo de backup.
      i. Selecione **Backup completo e backup de log** se quiser fazer backup de arquivos de banco de

dados e logs de transações.

ii. Selecione **Backup completo** se quiser fazer backup apenas dos arquivos do banco de dados.

iii. Selecione **Backup de Log** se quiser fazer backup apenas dos logs de transações.

iv. Selecione **Copiar somente backup** se quiser fazer backup de seus recursos usando outro aplicativo.

c. Na seção Configurações do grupo de disponibilidade, execute as seguintes ações:

i. Selecione Fazer backup na réplica de backup preferida se quiser fazer backup somente na réplica.

ii. Selecione a réplica do AG primário ou a réplica do AG secundário para o backup.

iii. Selecione a prioridade do backup.

6. Na página Snapshot e backup, execute as seguintes etapas:

a. Selecione a frequência do backup agendado.

b. Especifique as configurações de retenção dependendo do tipo de backup selecionado.

c. Se você quiser habilitar o backup do Azure NetApp Files , selecione **Habilitar backup** e especifique as configurações de retenção.

7. Na página Verificação, execute as seguintes etapas:

a. Na seção Executar verificação para os seguintes agendamentos de backup, selecione a frequência do agendamento.

b. Na seção Opções de verificação de consistência do banco de dados, execute as seguintes ações:

i. Selecione **Limitar a estrutura de integridade à estrutura física do banco de dados (PHYSICAL_ONLY)** para limitar a verificação de integridade à estrutura física do banco de dados e detectar páginas quebradas, falhas de soma de verificação e falhas comuns de hardware que afetam o banco de dados.

ii. Selecione **Suprimir todas as mensagens informativas (NO_INFOMSGS)** para suprimir todas as mensagens informativas.

Selecionado por padrão.

iii. Selecione **Exibir todas as mensagens de erro relatadas por objeto (ALL_ERRORMSGS)** para exibir todos os erros relatados por objeto.

iv. Selecione **Não verificar índices não agrupados (NOINDEX)** se não quiser verificar índices não agrupados.

O banco de dados SQL Server usa o Microsoft SQL Server Database Consistency Checker (DBCC) para verificar a integridade lógica e física dos objetos no banco de dados.

v. Selecione **Limitar as verificações e obter os bloqueios em vez de usar uma cópia de instantâneo do banco de dados interno (TABLOCK)** para limitar as verificações e obter os bloqueios em vez de usar um instantâneo do banco de dados interno.

c. Na seção **Backup de log**, selecione **Verificar backup de log após a conclusão** para verificar o backup de log após a conclusão.

d. Na seção **Configurações do script de verificação**, insira o caminho e os argumentos do prescript ou postscript que devem ser executados antes ou depois da operação de verificação, respectivamente.

8. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas de backup SQL

Um grupo de recursos é o contêiner ao qual você deve adicionar recursos que deseja fazer backup e proteger.

Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente. Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que deseja executar.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Insira um nome para o grupo de recursos.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos.
Use formato de nome personalizado para cópia do Snapshot	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.

4. Na página Recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Tipo de recurso**.
5. Selecione os recursos na seção **Recursos disponíveis** e clique na seta para a direita para movê-los para a seção **Recursos selecionados**.
6. Na página Políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Na coluna Configurar agendamentos, clique em * + * para a política que você deseja configurar.
   c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.
   d. Selecione o agendador do Microsoft SQL Server.
7. Na página Verificação, execute as seguintes etapas:
   a. Selecione o servidor de verificação.
   b. Selecione a política para a qual deseja configurar seu cronograma de verificação e clique em * + *.
   c. Selecione **Executar verificação após backup** ou **Executar verificação agendada**.
   d. Clique em **OK**.
8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.

9. Revise o resumo e clique em **Concluir**.

Fazer backup de bancos de dados do SQL Server em execução no Azure NetApp Files

Se um recurso ainda não fizer parte de nenhum grupo de recursos, você poderá fazer backup do recurso na página Recursos.

Antes de começar

Você deve criar um balanceador de carga se o Cluster de Failover do Windows do Azure não tiver um IP de cluster atribuído ou se não puder ser acessado pelo SnapCenter. O IP do balanceador de carga deve ser configurado e acessível a partir do SnapCenter Server.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recurso, selecione **Banco de dados**, **Instância** ou **Grupo de disponibilidade** na lista suspensa Exibir.
3. Na página Recurso, selecione **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.
4. Na página Políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Selecione * + * na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.
   c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione **OK**.

      policy_name é o nome da política que você selecionou.

   d. Selecione **Usar o agendador do Microsoft SQL Server** e, em seguida, selecione a instância do agendador na lista suspensa **Instância do agendador** associada à política de agendamento.
5. Na página Verificação, execute as seguintes etapas:
   a. Selecione o servidor de verificação.
   b. Selecione a política para a qual deseja configurar seu cronograma de verificação e clique em * + *.
   c. Selecione **Executar verificação após backup** ou **Executar verificação agendada**.
   d. Clique em OK.
6. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
7. Revise o resumo e clique em **Concluir**.
8. Selecione **Fazer backup agora**.
9. Na página Backup, execute as seguintes etapas:
   a. Se várias políticas estiverem associadas ao recurso, na lista suspensa **Política**, selecione a política que você deseja usar para backup.

b. Selecione **Verificar após backup**.

c. Selecione **Backup**.

10. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Fazer backup de grupos de recursos do SQL Server

Você pode fazer backup dos grupos de recursos que consistem em vários recursos. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.
3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e selecione **Fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
   a. Se várias políticas estiverem associadas ao grupo de recursos, na lista suspensa **Política**, selecione a política que você deseja usar para backup.
   b. Após o backup, selecione **Verificar** para verificar o backup sob demanda.
   c. Selecione **Backup**.
5. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Restaurar e recuperar bancos de dados SQL Server

Você pode usar o SnapCenter para restaurar bancos de dados SQL Server com backup. A restauração do banco de dados é um processo multifásico que copia todos os dados e páginas de log de um backup especificado do SQL Server para um banco de dados especificado.

Sobre esta tarefa

Você deve garantir que a instância de destino para restauração esteja configurada com um usuário do Active Directory que pertença ao domínio do Active Directory do SMB AD e tenha permissões para definir as permissões de arquivo adequadamente. Você deve configurar as credenciais no SnapCenter no nível da instância.

A autenticação SQL para instância de destino não será suportada para configurações SMB. A instância de destino deve ser configurada no SnapCenter com o usuário do Active Directory tendo as permissões necessárias.

Se a conta de serviço do SnapCenter Plug-in não for um usuário do Active Directory, ao executar a restauração no host alternativo, será necessário o usuário que tem controle total sobre os volumes de origem para que ele possa ser representado e executar a operação necessária.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista Exibir.

3. Selecione o banco de dados ou o grupo de recursos na lista.
4. Na exibição Gerenciar cópias, selecione **Backups** do sistema de armazenamento.
5. Selecione o backup da tabela e clique em  ícone.
6. Na página Escopo de restauração, selecione uma das seguintes opções:
   a. Selecione **Restaurar o banco de dados para o mesmo host onde o backup foi criado** se quiser restaurar o banco de dados para o mesmo servidor SQL onde os backups foram feitos.
   b. Selecione **Restaurar o banco de dados em um host alternativo** se desejar que o banco de dados seja restaurado em um servidor SQL diferente no mesmo host ou em um host diferente onde os backups são feitos.
7. Na página Escopo de Recuperação, selecione uma das seguintes opções:
   a. Selecione **Nenhum** quando precisar restaurar apenas o backup completo, sem nenhum log.
   b. Selecione a operação de restauração de backup atualizada **Todos os backups de log** para restaurar todos os backups de log disponíveis após o backup completo.
   c. Selecione **Por backups de log** para executar uma operação de restauração pontual, que restaura o banco de dados com base nos logs de backup até o log de backup com a data selecionada.
   d. Selecione **Por data específica até** para especificar a data e a hora após as quais os logs de transações não serão aplicados ao banco de dados restaurado.
   e. Se você selecionou **Todos os backups de log**, **Por backups de log** ou **Por data específica até** e os logs estiverem localizados em um local personalizado, selecione **Usar diretório de log personalizado** e especifique o local do log.
8. Na página Pré-operatório e Pós-operatório, especifique os detalhes necessários.
9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
10. Revise o resumo e clique em **Concluir**.
11. Monitore o processo de restauração usando a página **Monitor** > **Tarefas**.

Clonar backup do banco de dados SQL Server

Você pode usar o SnapCenter para clonar um banco de dados SQL usando o backup do banco de dados. Os clones criados são clones grossos e são criados no pool de capacidade pai.

Sobre esta tarefa

Você deve garantir que a instância de destino para clonagem esteja configurada com um usuário do Active Directory que pertença ao domínio do Active Directory do SMB AD e tenha permissões para definir as permissões de arquivo adequadamente. Você deve configurar as credenciais no SnapCenter no nível da instância.

A autenticação SQL para instância de destino não será suportada para configurações SMB. A instância de destino deve ser configurada no SnapCenter com o usuário do Active Directory tendo as permissões necessárias.

Se a conta de serviço do SnapCenter Plug-in não for um usuário do Active Directory, ao executar a clonagem, será necessário o usuário que tem controle total sobre os volumes de origem para que ele possa ser representado e executar a operação necessária.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados ou grupo de recursos.
4. Na página de exibição **Gerenciar cópias**, selecione o backup do sistema de armazenamento primário.
5. Selecione o backup e, em seguida, selecione *  *.
6. Na página **Opções de Clone**, forneça todos os detalhes necessários.
7. Na página Localização, selecione um local de armazenamento para criar um clone.

   Se os volumes ANF do banco de dados do SQL Server estiverem configurados em um pool de capacidade de QOS manual, especifique o QOS para os volumes clonados.

   Se o QOS para os volumes clonados não for especificado, o QOS do volume de origem será usado. Se o pool de capacidade de QOS automático for usado, o valor de QOS especificado será ignorado.

8. Na página Logs, selecione uma das seguintes opções:
   a. Selecione **Nenhum** se quiser clonar apenas o backup completo, sem nenhum registro.
   b. Selecione **Todos os backups de log** se quiser clonar todos os backups de log disponíveis datados após o backup completo.
   c. Selecione **Por backups de log até** se quiser clonar o banco de dados com base nos logs de backup que foram criados até o log de backup com a data selecionada.
   d. Selecione **Por data específica até** se não quiser aplicar os logs de transações após a data e hora especificadas.
9. Na página **Script**, insira o tempo limite do script, o caminho e os argumentos do prescript ou postscript que devem ser executados antes ou depois da operação de clonagem, respectivamente.
10. Na página **Notificação**, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais deseja enviar os e-mails.
11. Revise o resumo e selecione **Concluir**.
12. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Executar ciclo de vida do clone

Usando o SnapCenter, você pode criar clones de um grupo de recursos ou banco de dados. Você pode executar uma clonagem sob demanda ou agendar operações de clonagem recorrentes de um grupo de recursos ou banco de dados. Se você clonar um backup periodicamente, poderá usar o clone para desenvolver aplicativos, preencher dados ou recuperar dados.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista **Exibir**.
3. Selecione o banco de dados ou grupo de recursos.
4. Na página de exibição **Gerenciar cópias**, selecione o backup do sistema de armazenamento primário.
5.

Selecione o backup e, em seguida, selecione *  *.

6. Na página **Opções de Clone**, forneça todos os detalhes necessários.
7. Na página Localização, selecione um local de armazenamento para criar um clone.

   Se os volumes ANF do banco de dados do SQL Server estiverem configurados em um pool de capacidade de QOS manual, especifique o QOS para os volumes clonados.

   Se o QOS para os volumes clonados não for especificado, o QOS do volume de origem será usado. Se o pool de capacidade de QOS automático for usado, o valor de QOS especificado será ignorado.

8. Na página **Script**, insira o tempo limite do script, o caminho e os argumentos do prescript ou postscript que devem ser executados antes ou depois da operação de clonagem, respectivamente.
9. Na página Agendar, execute uma das seguintes ações:
   - Selecione **Executar agora** se quiser executar o trabalho de clonagem imediatamente.
   - Selecione **Configurar agendamento** quando quiser determinar com que frequência a operação de clonagem deve ocorrer, quando o agendamento de clonagem deve começar, em que dia a operação de clonagem deve ocorrer, quando o agendamento deve expirar e se os clones devem ser excluídos após o agendamento expirar.
10. Na página **Notificação**, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais deseja enviar os e-mails.
11. Revise o resumo e selecione **Concluir**.
12. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Proteja bancos de dados Oracle

Adicionar hosts e instalar o plug-in SnapCenter para banco de dados Oracle

Você pode usar a página Adicionar Host para adicionar hosts e, em seguida, instalar o Pacote de Plug-ins SnapCenter para Linux ou o Pacote de Plug-ins SnapCenter para AIX. Os plug-ins são instalados automaticamente nos hosts remotos.

Você pode adicionar um host e instalar pacotes de plug-in para um host individual ou para um cluster. Se você estiver instalando o plug-in em um cluster (Oracle RAC), o plug-in será instalado em todos os nós do cluster. Para o Oracle RAC One Node, você deve instalar o plug-in nos nós ativos e passivos.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se a guia **Hosts gerenciados** está selecionada.
3. Clique em **Adicionar**.
4. Na página Hosts, execute as seguintes ações:
   a. No campo Tipo de host, selecione o tipo de host.
   b. No campo Nome do host, insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host.
   c. No campo Credenciais, insira a credencial que você criou.
5. Na seção Selecionar plug-ins para instalar, selecione os plug-ins a serem instalados.

6. (Opcional) Clique em **Mais opções** e especifique os detalhes.
7. Clique em **Enviar**.
8. Verifique a impressão digital e clique em **Confirmar e Enviar**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós do cluster.

9. Monitore o progresso da instalação.

Crie políticas de backup para bancos de dados Oracle

Antes de usar o SnapCenter para fazer backup de recursos do banco de dados Oracle, você deve criar uma política de backup para o recurso ou grupo de recursos do qual deseja fazer backup.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Selecione Oracle Database na lista suspensa.
4. Clique em **Novo**.
5. Na página Nome, insira o nome e a descrição da política.
6. Na página Tipo de política, execute as seguintes etapas:
   a. Selecione * Azure NetApp Files* como o tipo de armazenamento.
   b. Selecione o tipo de backup como backup online ou offline.
   c. Se você quiser catalogar o backup usando o Oracle Recovery Manager (RMAN), selecione **Catalogar backup com o Oracle Recovery Manager (RMAN)**.
   d. Se você quiser remover logs de arquivo após o backup, selecione **Remover logs de arquivo após o backup**.
   e. Especifique as configurações de log de arquivo de exclusão.
7. Na página Snapshot e backup, execute as seguintes etapas:
   a. Selecione a frequência do backup agendado.
   b. Especifique as configurações de retenção.
   c. Se você quiser habilitar o backup do Azure NetApp Files , selecione **Habilitar backup** e especifique as configurações de retenção.
8. Na página Script, insira o caminho e os argumentos do prescript ou postscript que você deseja executar antes ou depois da operação de backup, respectivamente.
9. Na página Verificação, selecione o agendamento de backup para o qual você deseja executar a operação de verificação e insira o caminho e os argumentos do prescript ou postscript que você deseja executar antes ou depois da operação de verificação, respectivamente.
10. Revise o resumo e clique em **Concluir**.

Crie grupos de recursos e anexe políticas de backup do Oracle

Um grupo de recursos é o contêiner ao qual você deve adicionar recursos que deseja fazer backup e proteger.

Um grupo de recursos permite que você faça backup de todos os dados associados a um determinado aplicativo simultaneamente. Um grupo de recursos é necessário para qualquer trabalho de proteção de dados. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de trabalho de proteção de dados que deseja executar.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, clique em **Novo Grupo de Recursos**.
3. Na página Nome, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Insira um nome para o grupo de recursos.
Etiquetas	Insira um ou mais rótulos que ajudarão você a pesquisar posteriormente o grupo de recursos.
Use formato de nome personalizado para cópia do Snapshot	Marque esta caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.
Destino do arquivo de log de arquivamento	Especifique os destinos dos arquivos de log de arquivamento.

4. Na página Recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Tipo de recurso**.
5. Selecione os recursos na seção **Recursos disponíveis** e clique na seta para a direita para movê-los para a seção **Recursos selecionados**.
6. Na página Políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Na coluna Configurar agendamentos, clique em * + * para a política que você deseja configurar.
   c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e clique em **OK**.
7. Na página Verificação, execute as seguintes etapas:
   a. Selecione o servidor de verificação.
   b. Selecione a política para a qual deseja configurar seu cronograma de verificação e clique em * + .
   c. Selecione **Executar verificação após backup** ou **Executar verificação agendada**.
   d. Clique em **OK**.
8. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
9. Revise o resumo e clique em **Concluir**.

Fazer backup de bancos de dados Oracle em execução no Azure NetApp Files

Se um recurso ainda não fizer parte de nenhum grupo de recursos, você poderá fazer backup do recurso na página Recursos.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recurso, selecione **Banco de dados** na lista suspensa Exibir.
3. Na página Recurso, selecione **Usar formato de nome personalizado para cópia do Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome do Snapshot.
4. Na página Políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Selecione * + * na coluna Configurar agendamentos da política para a qual você deseja configurar um agendamento.
   c. Na caixa de diálogo Adicionar agendamentos para a política *nome_da_política*, configure o agendamento e selecione **OK**.
5. Na página Verificação, execute as seguintes etapas:
   a. Selecione o servidor de verificação.
   b. Selecione a política para a qual deseja configurar seu cronograma de verificação e clique em * + *.
   c. Selecione **Executar verificação após backup** ou **Executar verificação agendada**.
   d. Clique em OK.
6. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
7. Revise o resumo e clique em **Concluir**.
8. Selecione **Fazer backup agora**.
9. Na página Backup, execute as seguintes etapas:
   a. Se várias políticas estiverem associadas ao recurso, na lista suspensa **Política**, selecione a política que você deseja usar para backup.
   b. Clique em **Backup**.
10. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Fazer backup de grupos de recursos Oracle

Você pode fazer backup dos grupos de recursos que consistem em vários recursos. Uma operação de backup no grupo de recursos é executada em todos os recursos definidos no grupo de recursos.

Passos

1. No painel de navegação esquerdo, selecione **Recursos** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.

3. Na página Grupos de recursos, selecione o grupo de recursos que você deseja fazer backup e selecione **Fazer backup agora**.
4. Na página Backup, execute as seguintes etapas:
   a. Se várias políticas estiverem associadas ao grupo de recursos, na lista suspensa **Política**, selecione a política que você deseja usar para backup.
   b. Selecione **Backup**.
5. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Restaurar e recuperar bancos de dados Oracle

Em caso de perda de dados, você pode usar o SnapCenter para restaurar dados de um ou mais backups para seu sistema de arquivos ativo e, em seguida, recuperar o banco de dados.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista Exibir.
3. Selecione o banco de dados ou o grupo de recursos na lista.
4. Na exibição Gerenciar cópias, selecione **Backups** do sistema de armazenamento primário.
5. Selecione o backup da tabela e clique em *  *.
6. Na página Escopo de restauração, execute as seguintes tarefas:
   a. Selecione RAC se você selecionou um backup de um banco de dados no ambiente RAC.
   b. Execute as seguintes ações:
      i. Selecione **Todos os arquivos de dados** se quiser restaurar apenas os arquivos do banco de dados.
      ii. Selecione **Tablespaces** se quiser restaurar apenas os tablespaces.
      iii. Selecione **Refazer arquivos de log** se quiser restaurar os arquivos de log de refazer dos bancos de dados de espera do Data Guard ou do Active Data Guard.
      iv. Selecione **Bancos de dados conectáveis** e especifique os PDBs que deseja restaurar.
      v. Selecione **Tablespaces de banco de dados conectáveis (PDB)** e especifique o PDB e os tablespaces desse PDB que você deseja restaurar.
      vi. Selecione **Restaurar o banco de dados para o mesmo host onde o backup foi criado** se quiser restaurar o banco de dados para o mesmo servidor SQL onde os backups foram feitos.
      vii. Selecione **Restaurar o banco de dados em um host alternativo** se desejar que o banco de dados seja restaurado em um servidor SQL diferente no mesmo host ou em um host diferente onde os backups são feitos.
      viii. Selecione **Alterar estado do banco de dados, se necessário, para restauração e recuperação** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.
      ix. Selecione **Forçar restauração no local** se desejar executar a restauração no local em cenários onde novos arquivos de dados são adicionados após o backup ou quando LUNs são adicionados, excluídos ou recriados em um grupo de discos LVM.

7. Na página Escopo de Recuperação, selecione uma das seguintes opções:
   a. Selecione **Todos os registros** se quiser recuperar a última transação.
   b. Selecione **Até SCN (Número de alteração do sistema)** se quiser recuperar para um SCN específico.
   c. Selecione **Data e hora** se quiser recuperar para uma data e hora específicas.
   d. Selecione **Sem recuperação** se não quiser recuperar.
   e. Selecione **Especificar locais de log de arquivamento externo** se desejar especificar o local dos arquivos de log de arquivamento externo.
8. Na página Pré-operatório e Pós-operatório, especifique os detalhes necessários.
9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
10. Revise o resumo e clique em **Concluir**.
11. Monitore o progresso da operação clicando em **Monitorar** > **Trabalhos**.

Restaurar e recuperar tablespaces usando recuperação de ponto no tempo

Você pode restaurar um subconjunto de tablespaces que foram corrompidos ou descartados sem afetar os outros tablespaces no banco de dados. O SnapCenter usa o RMAN para executar a recuperação de ponto no tempo (PITR) dos tablespaces.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista Exibir.
3. Selecione o banco de dados do tipo instância única (multitenant).
4. Na exibição Gerenciar cópias, selecione **Backups** do sistema de armazenamento.

   Se o backup não estiver catalogado, você deve selecioná-lo e clicar em **Catálogo**.

5. Selecione o backup catalogado e clique em *  *.
6. Na página Escopo de restauração, execute as seguintes tarefas:
   a. Selecione **RAC** se você selecionou um backup de um banco de dados no ambiente RAC.
   b. Selecione **Tablespaces** se quiser restaurar apenas os tablespaces.
   c. Selecione **Alterar estado do banco de dados, se necessário, para restauração e recuperação** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.
7. Na página Escopo de Recuperação, selecione uma das seguintes opções:
   a. Selecione **Até SCN (Número de alteração do sistema)** se quiser recuperar para um SCN específico.
   b. Selecione **Data e hora** se quiser recuperar para uma data e hora específicas.
8. Na página Pré-operatório e Pós-operatório, especifique os detalhes necessários.
9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
10. Revise o resumo e clique em **Concluir**.
11. Monitore o processo de restauração usando a página **Monitor** > **Tarefas**.

Restaurar e recuperar banco de dados plugável usando recuperação de ponto no tempo

Você pode restaurar e recuperar um banco de dados conectável (PDB) que foi corrompido ou descartado sem afetar os outros PDBs no banco de dados do contêiner (CDB). O SnapCenter usa o RMAN para executar a recuperação de ponto no tempo (PITR) do PDB.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista Exibir.
3. Selecione o banco de dados do tipo instância única (multitenant).
4. Na exibição Gerenciar cópias, selecione **Backups** do sistema de armazenamento.

   Se o backup não estiver catalogado, você deve selecioná-lo e clicar em **Catálogo**.

5. Selecione o backup catalogado e clique em *  *.
6. Na página Escopo de restauração, execute as seguintes tarefas:
   a. Selecione **RAC** se você selecionou um backup de um banco de dados no ambiente RAC.
   b. Dependendo se você deseja restaurar o PDB ou os tablespaces em um PDB, execute uma das ações:
      - Selecione **Bancos de dados conectáveis (PDBs)** se quiser restaurar um PDB.
      - Selecione **Tablespaces de banco de dados conectáveis (PDB)** se desejar restaurar tablespaces em um PDB.
7. Na página Escopo de Recuperação, selecione uma das seguintes opções:
   a. Selecione **Até SCN (Número de alteração do sistema)** se quiser recuperar para um SCN específico.
   b. Selecione **Data e hora** se quiser recuperar para uma data e hora específicas.
8. Na página Pré-operatório e Pós-operatório, especifique os detalhes necessários.
9. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
10. Revise o resumo e clique em **Concluir**.
11. Monitore o processo de restauração usando a página **Monitor** > **Tarefas**.

Clonar backup do banco de dados Oracle

Você pode usar o SnapCenter para clonar um banco de dados Oracle usando o backup do banco de dados. Os clones criados são clones grossos e são criados no pool de capacidade pai.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista Exibir.
3. Selecione o banco de dados.
4. Na página de exibição Gerenciar cópias, selecione o backup do sistema de armazenamento primário.
5. Selecione o backup de dados e clique em *  *.

6. Na página Nome, selecione se deseja clonar um banco de dados (CDB ou não CDB) ou clonar um banco de dados conectável (PDB).
7. Na página Locais, especifique os detalhes necessários.

   Se os volumes ANF do banco de dados Oracle estiverem configurados em um pool de capacidade de QOS manual, especifique o QOS para os volumes clonados.

   Se o QOS para os volumes clonados não for especificado, o QOS do volume de origem será usado. Se o pool de capacidade de QOS automático for usado, o valor de QOS especificado será ignorado.

8. Na página Credenciais, execute uma das seguintes ações:
   a. Para Nome da credencial para o usuário sys, selecione a credencial a ser usada para definir a senha do usuário sys do banco de dados clone.
   b. Para Nome da credencial da instância ASM, selecione **Nenhum** se a autenticação do sistema operacional estiver habilitada para conexão com a instância ASM no host clone.

      Caso contrário, selecione a credencial do Oracle ASM configurada com o usuário “sys” ou um usuário com privilégio “sysasm” aplicável ao host clone.

9. Na página Pré-operações, especifique o caminho e os argumentos das prescrições e, na seção Configurações dos parâmetros do banco de dados, modifique os valores dos parâmetros do banco de dados pré-preenchidos que são usados para inicializar o banco de dados.
10. Na página Pós-Operações, **Recuperar banco de dados** e **Até Cancelar** são selecionados por padrão para executar a recuperação do banco de dados clonado.
    a. Se você selecionar **Até Cancelar**, o SnapCenter executará a recuperação montando o backup de log mais recente com a sequência ininterrupta de logs de arquivamento após o backup de dados que foi selecionado para clonagem.
    b. Se você selecionar **Data e hora**, o SnapCenter recuperará o banco de dados até uma data e hora especificadas.
    c. Se você selecionar **Até SCN**, o SnapCenter recuperará o banco de dados até um SCN especificado.
    d. Se você selecionar **Especificar locais de log de arquivamento externo**, o SnapCenter identificará e montará o número ideal de backups de log com base no SCN especificado ou na data e hora selecionadas.
    e. Por padrão, a caixa de seleção **Criar novo DBID** é selecionada para gerar um número exclusivo (DBID) para o banco de dados clonado, diferenciando-o do banco de dados de origem.

       Desmarque a caixa de seleção se quiser atribuir o DBID do banco de dados de origem ao banco de dados clonado. Nesse cenário, se você quiser registrar o banco de dados clonado no catálogo RMAN externo onde o banco de dados de origem já está registrado, a operação falhará.

    f. Marque a caixa de seleção **Criar arquivo temporário para espaço de tabela temporário** se desejar criar um arquivo temporário para o espaço de tabela temporário padrão do banco de dados clonado.
    g. Em **Inserir entradas SQL a serem aplicadas quando o clone for criado**, adicione as entradas SQL que você deseja aplicar quando o clone for criado.
    h. Em **Inserir scripts a serem executados após a operação de clonagem**, especifique o caminho e os argumentos do postscript que você deseja executar após a operação de clonagem.
11. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
12. Revise o resumo e selecione **Concluir**.

13. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Clonar um banco de dados plugável

Você pode clonar um banco de dados conectável (PDB) para um CDB de destino diferente ou igual no mesmo host ou em um host alternativo. Você também pode recuperar o PDB clonado para um SCN ou data e hora desejados.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Banco de dados** ou **Grupo de recursos** na lista Exibir.
3. Selecione o banco de dados do tipo instância única (multitenant).
4. Na página de exibição Gerenciar cópias, selecione o backup do sistema de armazenamento primário.
5. Selecione o backup e clique em *  *.
6. Na página Nome, selecione **PDB Clone** e especifique os outros detalhes.
7. Na página Locais, especifique os detalhes necessários.
8. Na página Pré-operações, especifique o caminho e os argumentos das prescrições e, na seção Configurações dos parâmetros do banco de dados, modifique os valores dos parâmetros do banco de dados pré-preenchidos que são usados para inicializar o banco de dados.
9. Na página Pós-Operações, **Até Cancelar** é selecionado por padrão para executar a recuperação do banco de dados clonado.
    a. Se você selecionar **Até Cancelar**, o SnapCenter executará a recuperação montando o backup de log mais recente com a sequência ininterrupta de logs de arquivamento após o backup de dados que foi selecionado para clonagem.
    b. Se você selecionar **Data e hora**, o SnapCenter recuperará o banco de dados até uma data e hora especificadas.
    c. Se você selecionar **Especificar locais de log de arquivamento externo**, o SnapCenter identificará e montará o número ideal de backups de log com base no SCN especificado ou na data e hora selecionadas.
    d. Por padrão, a caixa de seleção **Criar novo DBID** é selecionada para gerar um número exclusivo (DBID) para o banco de dados clonado, diferenciando-o do banco de dados de origem.

       Desmarque a caixa de seleção se quiser atribuir o DBID do banco de dados de origem ao banco de dados clonado. Nesse cenário, se você quiser registrar o banco de dados clonado no catálogo RMAN externo onde o banco de dados de origem já está registrado, a operação falhará.

    e. Marque a caixa de seleção **Criar arquivo temporário para espaço de tabela temporário** se desejar criar um arquivo temporário para o espaço de tabela temporário padrão do banco de dados clonado.
    f. Em **Inserir entradas SQL a serem aplicadas quando o clone for criado**, adicione as entradas SQL que você deseja aplicar quando o clone for criado.
    g. Em **Inserir scripts a serem executados após a operação de clonagem**, especifique o caminho e os argumentos do postscript que você deseja executar após a operação de clonagem.
10. Na página Notificação, na lista suspensa **Preferência de e-mail**, selecione os cenários nos quais você deseja enviar os e-mails.
11. Revise o resumo e selecione **Concluir**.

12. Monitore o progresso da operação selecionando **Monitor** > **Trabalhos**.

Gerenciar SnapCenter Server e plug-ins

Ver painel

Visão geral do painel

No painel de navegação esquerdo do SnapCenter , o Painel oferece uma primeira visão da integridade do seu sistema, incluindo atividade de trabalho recente, alertas, resumo de proteção, eficiência e uso de armazenamento, status de trabalhos do SnapCenter (backup, clone, restauração), status de configuração para hosts de cluster autônomos e do Windows, número de máquinas virtuais de armazenamento (SVMs) gerenciadas pelo SnapCenter e capacidade de licença.

As informações exibidas na visualização do Painel dependem da função atribuída ao usuário que está conectado no SnapCenter. Alguns conteúdos podem não ser exibidos se o usuário não tiver permissão para visualizar essas informações.

Em muitos casos, você pode ver mais informações sobre uma tela passando o mouse sobre **i**. Em alguns casos, as informações nas exibições do painel são vinculadas a informações detalhadas da fonte nas páginas da GUI do SnapCenter , como Recursos, Monitor e Relatórios.

Atividades de trabalho recentes

O bloco Atividades de trabalho recentes exibe a atividade de trabalho mais recente de todos os trabalhos de backup, restauração e clonagem aos quais você tem acesso. Os trabalhos nesta exibição têm um dos seguintes estados: Concluído, Aviso, Falha, Em execução, Na fila e Cancelado.

Passar o mouse sobre uma tarefa fornece mais informações. Você pode visualizar informações adicionais sobre o trabalho clicando em um número de trabalho específico, o que o redirecionará para a página Monitor. A partir daí, você pode obter detalhes do trabalho ou informações de registro e gerar um relatório específico para esse trabalho.

Clique em **Ver tudo** para visualizar um histórico de todos os trabalhos do SnapCenter .

Alertas

O bloco Alertas exibe os alertas críticos e de aviso não resolvidos mais recentes para os hosts e o SnapCenter Server.

A contagem total de alertas de categoria Crítica e Aviso é mostrada na parte superior do visor. Clicar nos totais Crítico ou de Aviso redireciona você para a página Alertas com o filtro específico aplicado na página Alertas.

Clicar em um alerta específico redireciona você para a página Alertas para obter detalhes sobre esse alerta. Clicar em **Ver tudo** na parte inferior da tela redireciona você para a página Alertas para obter uma lista de todos os alertas.

Resumo da proteção mais recente

O bloco Resumo de proteção mais recente fornece o status de proteção de todas as entidades às quais você tem acesso. Por padrão, a exibição é definida para fornecer o status de todos os plug-ins. Informações de status são fornecidas para recursos com backup no armazenamento primário como Snapshots e no

armazenamento secundário usando as tecnologias SnapMirror e SnapVault . A disponibilidade de informações de status de proteção para armazenamento secundário é baseada no tipo de plug-in selecionado.

Se você estiver usando uma política de proteção de mirror-vault, os contadores do resumo de proteção serão exibidos no gráfico de resumo do SnapVault e não no gráfico do SnapMirror .

O status de proteção para plug-ins individuais está disponível selecionando um plug-in no menu suspenso. Um gráfico de rosca mostra a porcentagem de recursos protegidos para o plug-in selecionado. Clicar em uma fatia de rosca redireciona você para a página **Relatórios** > **Plug-in**, que fornece um relatório detalhado de toda a atividade de armazenamento primário e secundário do plug-in especificado.

Relatórios sobre armazenamento secundário se aplicam somente ao SnapVault ; relatórios do SnapMirror não são suportados.

O SAP HANA fornece informações de status de proteção para armazenamento primário e secundário para Snapshots. Somente o status de proteção de armazenamento primário está disponível para backups baseados em arquivo.

Status de proteção	Armazenamento primário	Armazenamento secundário
Fracassado	Contagem de entidades que fazem parte de um Grupo de Recursos, onde o Grupo de Recursos executou um backup, mas o backup falhou.	Contagem de entidades com backups que falharam na transferência para um destino secundário.
Bem-sucedido	Contagem de entidades em um grupo de recursos, onde o backup do Grupo de Recursos foi feito com sucesso.	Contagem de entidades com backups que foram transferidos com sucesso para um destino secundário.
Não configurado	Contagem de entidades que não fazem parte de nenhum Grupo de Recursos e não foram submetidas a backup.	Contagem de entidades que fazem parte de um ou mais Grupos de Recursos que não estão configurados para backups a serem transferidos para um destino Secundário.
Não iniciado	Contagem de entidades que fazem parte de um Grupo de Recursos, mas nenhum backup foi executado.	Não aplicável.

Se você estiver usando o SnapCenter Server 4.2 e uma versão anterior do plug-in (anterior à 4.2) para criar backups, o bloco **Resumo da proteção mais recente** não exibirá o status de proteção do SnapMirror desses backups.

Empregos

O bloco Tarefas fornece um resumo das tarefas de backup, restauração e clonagem às quais você tem acesso. Você pode personalizar o período de qualquer relatório usando o menu suspenso. As opções de

período de tempo são fixadas em últimas 24 horas, últimos 7 dias e últimos 30 dias. O relatório padrão mostra os trabalhos de proteção de dados executados nos últimos 7 dias.

As informações de backup, restauração e clonagem são exibidas em gráficos de rosca. Clicar em uma fatia de donut redireciona você para a página Monitor com filtros de trabalho pré-aplicados à seleção.

Status do trabalho	Descrição
Fracassado	Contagem de trabalhos que falharam.
Aviso	Contagem de trabalhos que apresentaram erro.
Bem-sucedido	Contagem de trabalhos concluídos com sucesso.
Correndo	Contagem de trabalhos que estão em execução no momento.

Armazenar

O bloco Armazenamento exibe o armazenamento primário e secundário consumido por tarefas de proteção ao longo de um período de 90 dias, descreve graficamente as tendências de consumo e calcula a economia de armazenamento primário. As informações de armazenamento são atualizadas uma vez a cada 24 horas às 12h

O consumo total do dia, que inclui o número total de backups disponíveis no SnapCenter e o tamanho ocupado por esses backups, será exibido na parte superior da tela. Um backup pode ter vários Snapshots associados a ele e a contagem refletirá o mesmo. Isso se aplica tanto aos Snapshots primários quanto aos secundários. Por exemplo, você criou 10 backups, dos quais 2 foram excluídos devido à retenção de backup baseada em política e 1 backup foi explicitamente excluído por você. Assim, uma contagem de 7 backups será exibida junto com o tamanho ocupado por esses 7 backups.

O fator de economia de armazenamento para armazenamento primário é a proporção da capacidade lógica (economia de clones e instantâneos mais armazenamento consumido) em relação à capacidade física do armazenamento primário. Um gráfico de barras ilustra a economia de armazenamento.

O gráfico de linhas representa separadamente o consumo de armazenamento primário e secundário, dia a dia, durante um período contínuo de 90 dias. Passar o mouse sobre os gráficos fornece resultados detalhados dia a dia.

Se você usar o SnapCenter Server 4.2 e uma versão anterior do plug-in (anterior à 4.2) para criar backups, o bloco **Armazenamento** não exibirá o número de backups, o armazenamento consumido por esses backups, a economia de instantâneos, a economia de clones e o tamanho do instantâneo.

Configuração

O bloco Configuração fornece informações consolidadas de status para todos os hosts de cluster autônomos e do Windows ativos que o SnapCenter está gerenciando e aos quais você tem acesso. Isso inclui as informações de status do plug-in associadas a esses hosts.

Clicar no número ao lado de Hosts redireciona você para a seção Hosts gerenciados na página Hosts. A partir daí, você pode obter informações detalhadas sobre um host selecionado.

Além disso, esta exibição mostra a soma de SVMs ONTAP autônomos e SVMs ONTAP de cluster que o SnapCenter está gerenciando e aos quais você tem acesso. Clicar no número ao lado de SVM redireciona você para a página Sistemas de Armazenamento. A partir daí, você pode obter informações detalhadas sobre um SVM selecionado.

O estado de configuração do host é apresentado como vermelho (crítico), amarelo (aviso) e verde (ativo), juntamente com o número de hosts em cada estado. Mensagens de status são fornecidas para cada estado.

Status da configuração	Descrição
Atualização obrigatória	Contagem de hosts que estão executando plug-ins não suportados e precisam de uma atualização. Um plug-in não suportado não é compatível com esta versão do SnapCenter.
Migração obrigatória	Contagem de hosts que estão executando plug-ins não suportados e precisam de migração. Um plug-in não suportado não é compatível com esta versão do SnapCenter.
Nenhum plug-in instalado	Contagem de hosts adicionados com sucesso, mas os plug-ins precisam ser instalados ou a instalação dos plug-ins falhou.
Suspenso	Contagem de hosts cujas programações estão suspensas e em manutenção.
Parou	Contagem de hosts que estão ativos, mas os serviços de plug-in não estão em execução.
Host inativo	Contagem de hosts que estão inativos ou inacessíveis.
Atualização disponível (opcional)	Contagem de hosts onde uma versão mais recente do pacote de plug-in está disponível para atualização.
Migração disponível (opcional)	Contagem de hosts onde uma versão mais recente do plug-in está disponível para migração.
Configurar diretório de log	Contagem de hosts onde o diretório de log precisa ser configurado para que o SCSQL faça backup do log de transações.
Configurar plug-ins do VMware	Contagem de hosts onde o SnapCenter Plug-in for VMware vSphere precisa ser adicionado.
Desconhecido	Contagem de hosts que foram registrados, mas a instalação ainda não foi acionada.

Status da configuração	Descrição
Correndo	Contagem de hosts ativos e plug-ins em execução. E no caso de plug-ins SCSQL, o diretório de log e o hipervisor são configurados.
Instalando/Desinstalando plug-ins	Contagem de hosts onde a instalação ou desinstalação do plug-in está em andamento.

Como visualizar informações no painel

No painel de navegação esquerdo do SnapCenter , você pode visualizar vários blocos do Painel, ou exibições, juntamente com detalhes do sistema associados. O número de exibições disponíveis no Painel é fixo e não pode ser alterado. O conteúdo fornecido em cada exibição depende do controle de acesso baseado em função (RBAC).

Passos

1. No painel de navegação esquerdo, clique em **Painel**.
2. Clique nas áreas ativas em cada exibição para obter informações adicionais.

   Por exemplo, clicar em um gráfico de rosca em **Jobs** redireciona você para a página Monitor para obter mais informações sobre sua seleção. Clicar em um gráfico de rosca em **Resumo de proteção** redireciona você para a página Relatórios, que pode fornecer mais informações sobre sua seleção.

Solicitar relatórios de status dos trabalhos no painel

Você pode solicitar relatórios sobre tarefas de backup, restauração e clonagem na página Painel. Isso é útil se você quiser identificar o número total de trabalhos bem-sucedidos ou com falha no seu ambiente SnapCenter .

Passos

1. No painel de navegação esquerdo, clique em **Painel**
2. Localize o bloco Tarefas no Painel e selecione **Backup**, **Restaurar** ou **Clonar**.
3. Usando o menu suspenso, selecione o período para o qual deseja informações sobre os trabalhos: 24 horas, 7 dias ou 30 dias.

   Os sistemas exibem um gráfico de rosca cobrindo os dados.

4. Clique na fatia de rosca que representa as informações do trabalho para o qual você deseja um relatório.

   Ao clicar no gráfico de rosca, você será redirecionado da página Painel para a página Monitor. A página Monitor exibe os trabalhos com o status selecionado no gráfico de rosca.

5. Na lista da página Monitor, clique em um trabalho específico para selecioná-lo.
6. Na parte superior da página Monitor, clique em **Relatórios**.

Resultado

O relatório exibe informações somente para o trabalho selecionado. Você pode revisar o relatório ou baixá-lo para seu sistema local.

Solicitar relatórios do status de proteção no painel

Você pode solicitar detalhes de proteção para recursos gerenciados por plug-ins específicos usando o Painel. Somente backups de dados são considerados para o resumo de proteção de dados.

Passos

1. No painel de navegação esquerdo, clique em **Painel**.
2. Localize o bloco Resumo de proteção mais recente no Painel e use o menu suspenso para selecionar um plug-in.

   O Painel exibe um gráfico de donuts para recursos cujo backup foi feito no armazenamento primário e, se aplicável ao plug-in, um gráfico de donuts para recursos cujo backup foi feito no armazenamento secundário.

   Os relatórios de proteção de dados estão disponíveis apenas para tipos específicos de plug-ins. Não há suporte para especificar **Todos os plug-ins**.

3. Clique na fatia de rosca que representa o status para o qual você deseja um relatório.

   Ao clicar no gráfico de rosca, você será redirecionado da página Painel para os Relatórios e depois para a página Plug-in. O relatório exibe apenas o status do plug-in selecionado. Você pode revisar o relatório ou baixá-lo para seu sistema local.

   O redirecionamento para a página Relatórios do gráfico de donut do SnapMirror e do backup do SAP HANA baseado em arquivo não é suportado.

Gerenciar RBAC

O SnapCenter permite que você modifique funções, usuários e grupos.

Modificar uma função

Você pode modificar uma função do SnapCenter para remover usuários ou grupos e alterar as permissões associadas à função. É especialmente útil modificar funções quando você deseja alterar ou eliminar as permissões usadas por uma função inteira.

Antes de começar

Você deve ter efetuado login com a função "SnapCenterAdmin".

Você não pode modificar ou remover permissões para a função SnapCenterAdmin.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.

2. Na página Configurações, clique em **Funções**.
3. No campo Nome da função, clique na função que deseja modificar.
4. Selecione **Todos os membros desta função podem ver os objetos de outros membros** para permitir que outros membros da função vejam recursos como volumes e hosts depois de atualizarem a lista de recursos.

   Desmarque esta opção se não quiser que os membros desta função vejam objetos aos quais outros membros estão atribuídos.

   Quando esta opção está habilitada, não é necessário atribuir aos usuários acesso a objetos ou recursos se eles pertencerem à mesma função que o usuário que criou os objetos ou recursos.

5. Na página Detalhes da função, altere as permissões ou cancele a atribuição dos membros conforme necessário.
6. Clique em **Enviar**.

Modificar usuários e grupos

Você pode modificar usuários ou grupos do SnapCenter para alterar suas funções e ativos.

Antes de começar

Você deve estar logado como administrador do SnapCenter .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Usuários e acesso**.
3. Na lista Nome do usuário ou grupo, clique no usuário ou grupo que você deseja modificar.
4. Na página de detalhes do Usuário ou Grupo, altere funções e ativos.
5. Clique em **Enviar**.

Gerenciar hosts

Você pode adicionar hosts e instalar pacotes de plug-in do SnapCenter , adicionar um servidor de verificação, remover hosts, migrar tarefas de backup e atualizar o host para atualizar pacotes de plug-in ou adicionar novos pacotes de plug-in. Dependendo do plug-in que você estiver usando, você também pode provisionar discos, gerenciar compartilhamentos SMB, gerenciar grupos de iniciadores (igroups), gerenciar sessões iSCSI e migrar dados.

Você pode executar estas tarefas…	Para Microsoft Exchange Server	Para Microsoft SQL Server	Para Microsoft Windows	Para banco de dados Oracle	Para banco de dados SAP HANA	Para plug-ins suportados pela NetApp	Para Db2	Para PostgreSQL	Para MySQL
Adicionar hosts e instalar o pacote de plug-in	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Atualizar informações do ESXi para um host	Não	Sim	Não	Não	Não	Não	Não	Não	Não
Suspender agendamentos e colocar hosts em modo de manutenção	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Modifique hosts adicionando, atualizando ou removendo plug-ins	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Remover hosts do SnapCenter	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Você pode executar estas tarefas…	Para Microsoft Exchange Server	Para Microsoft SQL Server	Para Microsoft Windows	Para banco de dados Oracle	Para banco de dados SAP HANA	Para plug-ins suportados pela NetApp	Para Db2	Para PostgreSQL	Para MySQL
Iniciar serviços de plug-in (aplicável somente para plug-ins em execução no host Windows)	Sim	Sim	Sim	Não	Sim	Sim	Sim	Sim	Sim
Discos de provisionamento	Não	Não	Sim	Não	Não	Não	Não	Não	Não
Gerenciar compartilhamentos de PMEs	Não	Não	Sim	Não	Não	Não	Não	Não	Não
Gerenciar iGroups	Não	Não	Sim	Não	Não	Não	Não	Não	Não
Gerenciar sessões iSCSI	Não	Não	Sim	Não	Não	Não	Não	Não	Não

Atualizar informações da máquina virtual

Você deve atualizar as informações da sua máquina virtual quando as credenciais do VMware vCenter forem alteradas ou o host do banco de dados ou do sistema de arquivos for reiniciado. Atualizar as informações da sua máquina virtual no SnapCenter inicia a comunicação com o VMware vSphere vCenter e obtém as credenciais do vCenter.

Os discos baseados em RDM são gerenciados pelo SnapCenter Plug-in para Microsoft Windows, que é instalado no host do banco de dados. Para gerenciar RDMs, o SnapCenter Plug-in para Microsoft Windows se comunica com o servidor vCenter que gerencia o host do banco de dados.

Passos

1. No painel de navegação esquerdo do SnapCenter , clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Na página Hosts gerenciados, selecione o host que você deseja atualizar.
4. Clique em **Atualizar VM**.

Modificar hosts de plug-in

Após instalar um plug-in, você pode modificar os detalhes dos hosts do plug-in, se necessário. Você pode modificar credenciais, caminho de instalação, plug-ins, detalhes do diretório de log para o SnapCenter Plug-in para Microsoft SQL Server, conta de serviço gerenciada de grupo (gMSA) e a porta do plug-in.

Certifique-se de que a versão do plug-in seja a mesma que a versão do SnapCenter Server.

Sobre esta tarefa

- Você pode modificar uma porta de plug-in somente depois que o plug-in estiver instalado.

  Não é possível modificar a porta do plug-in enquanto as operações de atualização estiverem em andamento.

- Ao modificar uma porta de plug-in, você deve estar ciente dos seguintes cenários de reversão de porta:
  - Em uma configuração autônoma, se o SnapCenter não conseguir alterar a porta de um dos componentes, a operação falhará e a porta antiga será mantida para todos os componentes.

    Se a porta foi alterada para todos os componentes, mas um dos componentes não inicia com a nova porta, a porta antiga é mantida para todos os componentes. Por exemplo, se você quiser alterar a porta de dois plug-ins no host autônomo e o SnapCenter não conseguir aplicar a nova porta a um dos plug-ins, a operação falhará (com uma mensagem de erro apropriada) e a porta antiga será mantida para ambos os plug-ins.

  - Em uma configuração em cluster, se o SnapCenter não conseguir alterar a porta do plug-in instalado em um dos nós, a operação falhará e a porta antiga será mantida para todos os nós.

    Por exemplo, se o plug-in for instalado em quatro nós em uma configuração em cluster, e se a porta não for alterada para um dos nós, a porta antiga será mantida para todos os nós.

Quando os plug-ins são instalados com o gMSA, você pode modificá-los na janela **Mais Opções**. Quando plug-ins são instalados sem o gMSA, você pode especificar a conta do gMSA para usá-la como a conta de serviço do plug-in.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se **Hosts gerenciados** está selecionado na parte superior.
3. Selecione o host que você deseja modificar e modifique qualquer campo.

   Somente um campo pode ser modificado por vez.

4. Clique em **Enviar**.

Resultado

O host é validado e adicionado ao SnapCenter Server.

Iniciar ou reiniciar serviços de plug-in

Iniciar os serviços do plug-in SnapCenter permite que você inicie serviços se eles não estiverem em execução ou reinicie-os se estiverem em execução. Talvez você queira reiniciar os serviços após a manutenção ter sido realizada.

Você deve garantir que nenhuma tarefa esteja em execução ao reiniciar os serviços.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Na página Hosts gerenciados, selecione o host que você deseja iniciar.
4. Clique ícone e clique em **Iniciar serviço** ou **Reiniciar serviço**.

   Você pode iniciar ou reiniciar o serviço de vários hosts simultaneamente.

Suspender agendamentos para manutenção do host

Quando quiser impedir que o host execute qualquer tarefa agendada do SnapCenter , você pode colocá-lo no modo de manutenção. Você deve fazer isso antes de atualizar os plug-ins ou se estiver executando tarefas de manutenção nos hosts.

Não é possível suspender os agendamentos em um host que está inativo porque o SnapCenter não consegue se comunicar com esse host.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Na página Hosts gerenciados, selecione o host que você deseja suspender.
4. Clique no ícone e, em seguida, clique em **Suspender agendamento** para colocar o host deste plug-in no modo de manutenção.

   Você pode suspender a programação de vários hosts simultaneamente.

   Não é necessário interromper o serviço do plug-in primeiro. O serviço de plug-in pode estar em execução ou parado.

Resultado

Depois de suspender os agendamentos no host, a página Hosts gerenciados mostra **Suspenso** no campo Status geral do host.

Após concluir a manutenção do host, você pode retirá-lo do modo de manutenção clicando em **Ativar agendamento**. Você pode ativar a programação de vários hosts simultaneamente.

Operações suportadas pela página de Recursos

Você pode descobrir recursos e executar operações de proteção de dados na página Recursos. As operações que você pode executar variam de acordo com o plug-in que você está usando para gerenciar seus recursos.

Na página Recursos, você pode executar as seguintes tarefas:

Você pode executar estas tarefas…	Para Microsoft Exchange Server	Para Microsoft SQL Server	Para Microsoft Windows	Para banco de dados Oracle	Para banco de dados SAP HANA
Determinar se há recursos disponíveis para backup	Sim	Sim	Sim	Sim	Sim
Executar backup sob demanda de um recurso	Sim	Sim	Sim	Sim	Sim
Restaurar a partir de backups	Sim	Sim	Sim	Sim	Sim
Clonar backups	Não	Sim	Sim	Sim	Sim
Gerenciar backups	Sim	Sim	Sim	Sim	Sim
Gerenciar clones	Não	Sim	Sim	Sim	Sim
Gerenciar políticas	Sim	Sim	Sim	Sim	Sim
Gerenciar conexões de armazenamento	Sim	Sim	Sim	Sim	Sim
Montar backups	Não	Não	Não	Sim	Não
Desmontar backups	Não	Não	Não	Sim	Não
Ver detalhes	Sim	Sim	Sim	Sim	Sim

Gerenciar políticas

Você pode desanexar políticas de um recurso ou grupo de recursos, modificar, excluir, visualizar e copiar.

Modificar políticas

Você pode modificar as opções de replicação, as configurações de retenção de instantâneos, a contagem de novas tentativas de erro ou as informações de scripts enquanto uma política estiver anexada a um recurso ou grupo de recursos. Você pode modificar o tipo de agendamento (frequência) somente depois de desanexar uma política.

Sobre esta tarefa

Modificar o tipo de agendamento em uma política requer etapas adicionais porque o SnapCenter Server registra o tipo de agendamento somente no momento em que a política é anexada a um recurso ou grupo de recursos.

Se você quiser…	Então…
Adicionar um tipo de programação adicional	Crie uma nova política e anexe-a aos recursos ou grupos de recursos necessários. Por exemplo, se uma política de grupo de recursos especificar apenas backups de hora em hora e você quiser adicionar backups diários também, poderá criar uma política com um tipo de agendamento diário e adicioná-la ao grupo de recursos. O grupo de recursos teria então duas políticas: horária e diária.
Remover ou alterar um tipo de programação	Execute o seguinte: 1. Desanexe a política de cada recurso e grupo de recursos que usa essa política. 2. Modifique o tipo de programação. 3. Anexe a política novamente a todos os recursos e grupos de recursos. Por exemplo, se uma política especifica backups de hora em hora e você deseja alterá-la para backups diários, você deve desanexar a política primeiro.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Selecione a política e clique em **Modificar**.
4. Modifique as informações e clique em **Concluir**.

Políticas de desanexação

Você pode desanexar políticas de um recurso ou grupo de recursos sempre que não quiser mais que essas políticas controlem a proteção de dados dos recursos. Você deve desanexar uma política antes de excluí-la ou antes de modificar o tipo de agendamento.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.
3. Selecione o grupo de recursos e clique em **Modificar grupo de recursos**.
4. Na página Políticas do assistente Modificar Grupo de Recursos, na lista suspensa, desmarque a marca de seleção ao lado das políticas que deseja desanexar.
5. Faça quaisquer modificações adicionais no grupo de recursos no restante do assistente e clique em **Concluir**.

Excluir políticas

Se você não precisar mais de políticas, talvez seja necessário excluí-las.

Antes de começar

Você deve desanexar a política do recurso ou grupos de recursos se ela estiver associada a qualquer recurso ou grupo de recursos.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Políticas**.
3. Selecione a política e clique em **Excluir**.
4. Clique em **Sim**.

Gerenciar grupos de recursos

Você pode executar várias operações em grupos de recursos.

Você pode executar as seguintes tarefas relacionadas a grupos de recursos:

- Modifique um grupo de recursos selecionando-o e clicando em **Modificar grupo de recursos** para editar as informações fornecidas ao criar o grupo de recursos.

  Você pode alterar o cronograma enquanto modifica o grupo de recursos. Entretanto, para alterar o tipo de programação, você deve modificar a política.

  Se você remover recursos de um grupo de recursos, as configurações de retenção de backup definidas nas políticas atualmente anexadas ao grupo de recursos continuarão a ser aplicadas aos recursos removidos.

- Crie um backup de um grupo de recursos.
- Crie um clone de um backup.

Você pode clonar backups existentes de SQL, Oracle, sistemas de arquivos Windows, aplicativos personalizados e recursos ou grupos de recursos de banco de dados SAP HANA.

- Crie um clone de um grupo de recursos.

  Esta operação é suportada somente para grupos de recursos SQL (que contêm somente bancos de dados). Você pode configurar um cronograma para clonar um grupo de recursos (ciclo de vida do clone).

- Impedir que operações agendadas em grupos de recursos sejam iniciadas.
- Excluir um grupo de recursos.

Parar e retomar operações em grupos de recursos

Você pode desabilitar temporariamente o início de operações agendadas em um grupo de recursos. Mais tarde, quando quiser, você pode habilitar essas operações.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.
3. Selecione o grupo de recursos e clique em **Manutenção**.
4. Clique em **OK**.

Se você quiser retomar as operações no grupo de recursos que colocou no modo de manutenção, selecione o grupo de recursos e clique em **Produção**.

Excluir grupos de recursos

Você pode excluir um grupo de recursos se não precisar mais proteger os recursos nele contidos. Você deve garantir que os grupos de recursos sejam excluídos antes de remover plug-ins do SnapCenter.

Sobre esta tarefa

Você deve excluir manualmente todos os clones criados para qualquer um dos recursos no grupo de recursos. Opcionalmente, você pode forçar a exclusão de todos os backups, metadados, políticas e instantâneos associados ao grupo de recursos.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione **Grupo de recursos** na lista **Exibir**.
3. Selecione o grupo de recursos e clique em **Excluir**.
4. Opcional: marque a caixa de seleção **Excluir backups e desanexar políticas associadas a este grupo de recursos** para remover todos os backups, metadados, políticas e instantâneos associados ao grupo de recursos.
5. Clique em **OK**.

Gerenciar backups

Você pode renomear e excluir backups. Você também pode excluir vários backups

simultaneamente.

Renomear backups

Você pode renomear os backups se quiser fornecer um nome melhor para melhorar a capacidade de pesquisa.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso ou grupo de recursos na lista.

   A página de topologia de recurso ou grupo de recursos é exibida. Se o recurso ou grupo de recursos não estiver configurado para proteção de dados, o assistente de proteção será exibido em vez da página de topologia.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primários.

   Não é possível renomear os backups que estão no sistema de armazenamento secundário.

   Se você catalogou os backups de bancos de dados Oracle usando o Oracle Recovery Manager (RMAN), não poderá renomear esses backups catalogados.

5. Selecione o backup e clique em  .
6. No campo **Renomear backup como**, insira um novo nome e clique em **OK**.

Excluir backups

Você pode excluir backups se não precisar mais deles para outras operações de proteção de dados.

Antes de começar

Você deve ter excluído os clones associados antes de excluir um backup.

Se um backup estiver associado a um recurso clonado, você não poderá excluí-lo.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso ou grupo de recursos na lista.

   A página de topologia de recurso ou grupo de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Backups** dos sistemas de armazenamento primários.

   Você não pode excluir os backups que estão no sistema de armazenamento secundário.

5. Selecione o backup e clique em  .

   Se você estiver excluindo um backup de banco de dados SAP HANA, os catálogos SAP HANA associados

ao backup também serão excluídos.

> Se o último backup restante for excluído, as entradas do catálogo HANA associadas não poderão ser excluídas.

6. Clique em **OK**.

> Se você tiver alguns backups de banco de dados obsoletos no SnapCenter que não tenham backups correspondentes no sistema de armazenamento, você deve usar o comando remove-smbackup para limpar essas entradas de backup obsoletas. Se os backups obsoletos foram catalogados, eles serão descatalogados do banco de dados do catálogo de recuperação.

Remover proteção

Remover proteção exclui todos os backups e desvincula todas as políticas. Antes de remover a proteção, você deve garantir que os backups não estejam montados e que nenhum clone esteja associado ao backup.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso ou grupo de recursos na lista.

   A página de topologia de recurso ou grupo de recursos é exibida.

4. Selecione o backup e clique em **Remover proteção**.

Excluir clones

Você pode excluir clones se achar que eles não são mais necessários.

Sobre esta tarefa

Você não pode excluir clones que atuam como fonte para outros clones.

Por exemplo, se o banco de dados de produção for db1, o clone1 do banco de dados será clonado do backup do db1 e, posteriormente, o clone1 será protegido. O banco de dados clone2 é clonado do backup do clone1. Se você decidir excluir o clone1, primeiro deverá excluir o clone2 e depois excluir o clone1.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Na página Recursos, selecione o recurso ou grupo de recursos na lista suspensa **Exibir**.
3. Selecione o recurso ou grupo de recursos na lista.

   A página de topologia do recurso ou do grupo de recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **Clones** dos sistemas de armazenamento primário ou secundário (espelhado ou replicado).

5. Selecione o clone e clique em .

   Se você estiver excluindo clones do banco de dados SAP HANA, na página Excluir clone, execute as seguintes ações:

   a. No campo **Pre clone delete**, insira os comandos que devem ser executados antes de excluir o clone.
   b. No campo **Desmontar**, digite o comando para desmontar o clone antes de excluí-lo.

6. Clique em **OK**.

Depois que você terminar

Às vezes, os sistemas de arquivos não são excluídos. Você deve aumentar o valor do parâmetro CLONE_DELETE_DELAY executando o seguinte comando: `./sccli Set-SmConfigSettings`

> O parâmetro CLONE_DELETE_DELAY especifica o número de segundos a aguardar após a conclusão da exclusão do clone do aplicativo e antes de iniciar a exclusão do sistema de arquivos.

Após modificar o valor do parâmetro, reinicie o serviço SnapCenter Plug-in Loader (SPL).

Monitorar trabalhos, agendamentos, eventos e registros

Você pode monitorar o progresso dos seus trabalhos, obter informações sobre trabalhos agendados e revisar eventos e logs na página Monitorar.

Monitorar trabalhos

Você pode visualizar informações sobre trabalhos de backup, clonagem, restauração e verificação do SnapCenter . Você pode filtrar esta visualização com base na data de início e término, tipo de trabalho, grupo de recursos, política ou plug-in do SnapCenter . Você também pode obter detalhes adicionais e arquivos de log para trabalhos específicos.

Você também pode monitorar trabalhos relacionados às operações do SnapMirror e do SnapVault .

> Você pode monitorar somente os trabalhos que criou e que são relevantes para você, a menos que tenha a função de administrador do SnapCenter ou outra função de superusuário atribuída a você.

Você pode executar as seguintes tarefas relacionadas aos trabalhos de monitoramento:

- Monitore operações de backup, clonagem, restauração e verificação.
- Veja detalhes e relatórios do trabalho.
- Interromper uma tarefa agendada.

Gerenciar tarefas de backup agendadas

A partir do lançamento do SnapCenter 6.0.1, um novo parâmetro **JobConcurrencyThreshold** foi introduzido, definindo um limite para o número de trabalhos agendados que podem ser executados a qualquer momento. Isso permite que você controle o número de backups que deseja executar com base na configuração de hardware do seu sistema.

O valor padrão atribuído a **JobConcurrencyThreshold** é 0 e está desabilitado. Você pode habilitar atribuindo um valor, caso observe degradação de desempenho durante a janela de backup agendada.

> Se você habilitar **JobConcurrencyThreshold** para gerenciar trabalhos simultâneos, o SnapCenter não permitirá que você controle a ordem dos backups e os backups poderão não ser disparados no mesmo horário especificado no agendamento.

Passos

1. Defina o valor do parâmetro *JobConcurrencyThreshold* localizado em *C:\Program Files\ NetApp\ SnapCenter WebApp\ SnapManager.Web.UI.dll.config*.
2. Recicle o pool de aplicativos do SnapCenter clicando em IIS > Pools de aplicativos > SnapCenter > Reiniciar.
3. Reinicie o serviço Web SnapCenter clicando em IIS > Sites > SnapCenter > Reiniciar.

Gerenciar trabalhos obsoletos

Trabalhos obsoletos são criados a partir de interrupções no SnapCenter ou de atualizações inadequadas de trabalhos. A partir do lançamento do SnapCenter 6.0.1, um cronograma predefinido é introduzido para limpar esses trabalhos obsoletos que ficam presos por mais de 72 horas. Você pode alterar a frequência da programação editando o parâmetro configurável **CleanUpStaleJobsIntervalHours**.

Você pode acionar a limpeza sob demanda executando a programação em **Monitor** > **Agendamentos** > **SnapCenter_StaleJobCleanUp**.

Passos

1. Defina o valor do parâmetro *CleanUpStaleJobsIntervalHours* localizado em *C:\Program Files\ NetApp\ SnapCenter WebApp\ SnapManager.Web.UI.dll.config*.
2. Recicle o pool de aplicativos do SnapCenter clicando em IIS > Pools de aplicativos > SnapCenter > Reiniciar.
3. Reinicie o serviço Web SnapCenter clicando em IIS > Sites > SnapCenter > Reiniciar.

Monitorar cronogramas

Talvez você queira visualizar os cronogramas atuais para determinar quando a operação começa, quando foi executada pela última vez e quando será executada novamente. Você também pode determinar o host no qual a operação é executada, juntamente com o grupo de recursos e informações de política da operação.

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **Agendamentos**.
3. Selecione o grupo de recursos e o tipo de programação.
4. Veja a lista de operações programadas.

Monitorar eventos

Você pode visualizar uma lista de eventos do SnapCenter no sistema, como quando um usuário cria um grupo de recursos ou quando o sistema inicia atividades, como a criação de um backup agendado. Talvez você queira visualizar eventos para determinar se uma operação, como um backup ou uma restauração, está em andamento.

Sobre esta tarefa

Todas as informações do trabalho aparecem na página Eventos. Por exemplo, quando um trabalho de backup é iniciado, um evento “backup start” aparece. Quando o backup for concluído, um evento “backup concluído” será exibido.

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **Eventos**.
3. (Opcional) Na caixa Filtro, insira a data de início ou término, a categoria do evento (como backup, grupo de recursos ou política) e o nível de gravidade e clique em **Aplicar**. Como alternativa, insira caracteres na caixa de pesquisa.
4. Veja a lista de eventos.

Registros de monitoramento

Você pode visualizar e baixar logs do SnapCenter Server, logs do agente de host do SnapCenter e logs de plug-ins. Talvez você queira visualizar os logs para ajudar na solução de problemas.

Sobre esta tarefa

Você pode filtrar os logs para mostrar apenas um nível de gravidade de log específico:

- Depurar
- Informações
- Avisar
- Erro
- Fatal

Você também pode obter logs de nível de tarefa, por exemplo, logs que ajudam a solucionar o motivo de uma falha de tarefa de backup. Para logs de nível de trabalho, use a opção **Monitor** > **Jobs**.

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Trabalhos, selecione um trabalho e clique em Baixar logs.

   A pasta compactada baixada contém os logs de trabalho e os logs comuns. O nome da pasta compactada contém o ID do trabalho e o tipo de trabalho selecionado.

3. Na página Monitor, clique em **Logs**.
4. Selecione o tipo de log, host e instância.

   Se você selecionar o tipo de log como **plugin**, poderá selecionar um host ou um plug-in do SnapCenter . Isso não é possível se o tipo de log for **servidor**.

5. Para filtrar os logs por uma fonte, mensagem ou nível de log específico, clique no ícone de filtro na parte superior do título da coluna.

   Para mostrar todos os logs, escolha **Maior ou igual a** como `Debug` nível.

6. Clique em **Atualizar**.
7. Veja a lista de logs.
8. Clique em **Download** para baixar os logs.

   A pasta compactada baixada contém os logs de trabalho e os logs comuns. O nome da pasta compactada contém o ID do trabalho e o tipo de trabalho selecionado.

Em configurações grandes para desempenho ideal, você deve definir as configurações de log do SnapCenter para o nível mínimo usando o cmdlet do PowerShell.

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10
-JobLogsMaxFileSize 10MB -Server
```

Para acessar informações de integridade ou configuração após a conclusão de um trabalho de failover, execute o cmdlet `Get-SmRepositoryConfig` .

Remover trabalhos e logs do SnapCenter

Você pode remover trabalhos e logs de backup, restauração, clonagem e verificação do SnapCenter. O SnapCenter armazena logs de tarefas bem-sucedidas e com falha indefinidamente, a menos que você os remova. Talvez você queira removê-los para reabastecer o armazenamento.

Sobre esta tarefa

Não deve haver nenhuma tarefa em operação no momento. Você pode remover um trabalho específico fornecendo um ID de trabalho ou pode remover trabalhos dentro de um período especificado.

Não é necessário colocar o host no modo de manutenção para remover trabalhos.

Passos

1. Inicie o PowerShell.
2. No prompt de comando, digite: `Open-SMConnection`
3. No prompt de comando, digite: `Remove-SmJobs`
4. No painel de navegação esquerdo, clique em **Monitor**.
5. Na página Monitor, clique em **Trabalhos**.
6. Na página Trabalhos, revise o status do trabalho.

Informações relacionadas

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Visão geral dos recursos de relatórios do SnapCenter

O SnapCenter fornece uma variedade de opções de relatórios que permitem monitorar e gerenciar a integridade do sistema e o sucesso da operação.

Tipo de relatório	Descrição
Relatório de backup	O Relatório de backup fornece dados gerais sobre tendências de backup para seu ambiente SnapCenter , a taxa de sucesso do backup e algumas informações sobre cada backup executado durante o período especificado. Se um backup for excluído, o relatório não exibirá nenhuma informação de status para o backup excluído. O Relatório de detalhes de backup fornece informações detalhadas sobre uma tarefa de backup especificada e lista os recursos cujo backup foi feito com sucesso e aqueles que falharam.
Relatório de Clone	O Relatório de Clone fornece dados gerais sobre tendências de clone para seu ambiente SnapCenter , a taxa de sucesso de clone e algumas informações sobre cada trabalho de clone executado durante o período especificado. Se um clone for excluído, o relatório não exibirá nenhuma informação de status para o clone excluído. O Relatório de Detalhes do Clone fornece detalhes sobre o clone especificado, o host do clone e o status da tarefa do trabalho do clone. Se uma tarefa falhar, o Relatório de Detalhes do Clone exibirá informações sobre a falha.
Relatório de restauração	O Relatório de restauração fornece informações gerais sobre tarefas de restauração. O Relatório de Detalhes da Restauração fornece detalhes sobre um trabalho de restauração especificado, incluindo nome do host, nome do backup, início e duração do trabalho e o status de tarefas individuais. Se uma tarefa falhar, o Relatório de Detalhes da Restauração exibirá informações sobre a falha.
Relatório de Proteção	Esses relatórios fornecem detalhes de proteção para recursos gerenciados por todas as instâncias do plug-in SnapCenter . Este relatório fornece detalhes de proteção para recursos gerenciados por todas as instâncias de plug-in. Você pode ver uma visão geral, detalhes de recursos desprotegidos, recursos que não foram submetidos a backup quando o relatório foi gerado, recursos de um grupo de recursos para os quais as operações de backup falharam e o status do SnapVault .

Tipo de relatório	Descrição
Relatório agendado	Esses relatórios são programados para serem executados periodicamente, como diariamente, semanalmente ou mensalmente. Os relatórios são gerados automaticamente na data e hora especificadas e são enviados às respectivas pessoas por e-mail. Você pode habilitar, desabilitar, modificar ou excluir as programações. O agendamento habilitado pode ser executado sob demanda clicando no botão **Executar agora**. O administrador pode executar qualquer agendamento, mas o relatório gerado conterá dados com base na permissão fornecida pelo usuário que criou o agendamento. Qualquer outro usuário que não seja Administrador poderá ver ou modificar a programação com base em sua permissão. Se a opção Todos os membros desta função podem ver os objetos de outros membros estiver selecionada na página Adicionar função, outros membros da função poderão ver e modificar.

Relatórios de acesso

Você pode usar o Painel do SnapCenter para obter uma visão geral rápida da integridade do seu sistema. No Painel, você pode obter mais detalhes. Alternativamente, você pode acessar os relatórios detalhados diretamente.

Você pode acessar relatórios por um dos seguintes métodos:

- No painel de navegação esquerdo, clique em **Painel** e, em seguida, clique no gráfico de pizza **Resumo da última proteção** para ver mais detalhes na página Relatórios.
- No painel de navegação esquerdo, clique em **Relatórios**.

Filtre seu relatório

Talvez você queira filtrar os dados do seu relatório de acordo com uma série de parâmetros, dependendo do nível de detalhe e do período de tempo das informações necessárias.

Passos

1. No painel de navegação esquerdo, clique em **Relatórios**.
2. Se a exibição de parâmetros não for exibida, clique no ícone **Alternar área de parâmetros** na barra de ferramentas do relatório.
3. Especifique o intervalo de tempo para o qual você deseja executar seu relatório. + Se você omitir a data final, você recuperará todas as informações disponíveis.
4. Filtre as informações do seu relatório com base em qualquer um dos seguintes critérios:
    - Grupo de recursos
    - Hospedar
    - Política

- Recurso
- Status
- Nome do plug-in

5. Clique em **Aplicar**.

Exportar ou imprimir relatórios

Exportar relatórios do SnapCenter permite que você visualize o relatório em uma variedade de formatos alternativos. Você também pode imprimir relatórios.

Passos

1. No painel de navegação esquerdo, clique em **Relatórios**.
2. Na barra de ferramentas de relatórios, execute uma das seguintes ações:
   - Clique no ícone **Alternar visualização de impressão** para visualizar um relatório para impressão.
   - Selecione um formato na lista suspensa do ícone **Exportar** para exportar um relatório para um formato alternativo.
3. Para imprimir um relatório, clique no ícone **Imprimir**.
4. Para visualizar um resumo de relatório específico, role até a seção apropriada do relatório.

Defina o servidor SMTP para notificações por e-mail

Você pode especificar o servidor SMTP a ser usado para enviar relatórios de tarefas de proteção de dados para você ou para outras pessoas. Você também pode enviar um e-mail de teste para verificar a configuração. As configurações são aplicadas globalmente para qualquer trabalho do SnapCenter para o qual você configura a notificação por e-mail.

Esta opção configura o servidor SMTP para enviar todos os relatórios de tarefas de proteção de dados. No entanto, se você quiser que atualizações regulares de tarefas de proteção de dados do SnapCenter para um recurso específico sejam enviadas a você mesmo ou a outras pessoas para que você possa monitorar o status dessas atualizações, você pode configurar a opção de enviar os relatórios do SnapCenter por e-mail quando estiver criando um grupo de recursos.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Configurações globais**.
3. Digite o servidor SMTP e clique em **Salvar**.
4. Para enviar um e-mail de teste, insira o endereço de e-mail de onde e para onde você enviará o e-mail, insira o assunto e clique em **Enviar**.

Configurar a opção de enviar relatórios por e-mail

Se você quiser que atualizações regulares de tarefas de proteção de dados do SnapCenter sejam enviadas para você ou para outras pessoas para poder monitorar o status dessas atualizações, você pode configurar a opção de enviar os relatórios do SnapCenter por e-mail ao criar um grupo de recursos.

Antes de começar

Você deve ter configurado seu servidor SMTP na página Configurações globais em Configurações.

Passos

1. No painel de navegação esquerdo, clique em **Recursos** e selecione o plug-in apropriado na lista.
2. Selecione o tipo de recurso que deseja visualizar e clique em **Novo grupo de recursos** ou selecione um grupo de recursos existente e clique em **Modificar** para configurar relatórios por e-mail para um grupo de recursos existente.
3. No painel Notificação do assistente Novo Grupo de Recursos, selecione no menu suspenso se deseja receber relatórios sempre, em caso de falha ou em caso de falha ou aviso.
4. Insira o endereço de onde o e-mail foi enviado, o endereço para o qual o e-mail foi enviado e o assunto do e-mail.

Gerenciar o repositório do SnapCenter Server

Informações relacionadas a várias operações realizadas no SnapCenter são armazenadas no repositório de banco de dados do SnapCenter Server. Você deve criar backups do repositório para proteger o SnapCenter Server contra perda de dados.

O repositório do SnapCenter Server às vezes é chamado de banco de dados NSM.

Pré-requisitos para proteger o repositório SnapCenter

Seu ambiente deve atender a certos pré-requisitos para proteger o repositório do SnapCenter .

- Gerenciando conexões de máquina virtual de armazenamento (SVM)

  Você deve configurar as credenciais de armazenamento.

- Provisionamento de hosts

  Pelo menos um disco de armazenamento NetApp deve estar presente no host do repositório SnapCenter . Se um disco NetApp não estiver presente no host do repositório SnapCenter , você deverá criar um.

  Para obter detalhes sobre como adicionar hosts, configurar conexões SVM e provisionar hosts, consulte as instruções de instalação.

- Provisionamento de iSCSI LUN ou VMDK

  Para configuração de alta disponibilidade (HA), você pode provisionar um LUN iSCSI ou um VMDK em um dos SnapCenter Servers.

Faça backup do repositório SnapCenter

Fazer backup do repositório do SnapCenter Server ajuda a protegê-lo contra perda de dados. Você pode fazer backup do repositório executando o cmdlet *Protect-SmRepository*.

Sobre esta tarefa

O cmdlet *Protect-SmRepository* realiza as seguintes tarefas:

- Cria um grupo de recursos e uma política
- Cria um agendamento de backup para o repositório SnapCenter

Passos

1. Inicie o PowerShell.
2. No host do SnapCenter Server, estabeleça uma sessão usando o cmdlet *Open-SmConnection* e insira suas credenciais.
3. Faça backup do repositório usando o cmdlet *Protect-SmRepository* e os parâmetros necessários.

Ver backups do repositório SnapCenter

Você pode exibir uma lista de backups do repositório de banco de dados do SnapCenter Server executando o cmdlet *Get-SmRepositoryBackups*.

Os backups do repositório são criados de acordo com o agendamento especificado no cmdlet *Protect-SmRepository*.

Passos

1. Inicie o PowerShell.
2. No prompt de comando, insira o seguinte cmdlet e forneça credenciais para se conectar ao SnapCenter Server: *Open-SMConnection*
3. Liste todos os backups de banco de dados SnapCenter disponíveis usando o cmdlet *Get-SmRepositoryBackups*.

Restaurar o repositório do banco de dados SnapCenter

Você pode restaurar o repositório SnapCenter executando o cmdlet *Restore-SmRepositoryBackup*.

Ao restaurar o repositório do SnapCenter , outras operações do SnapCenter em execução serão afetadas porque, durante a operação de restauração, o banco de dados do repositório não estará acessível.

Passos

1. Inicie o PowerShell.
2. No prompt de comando, insira o seguinte cmdlet e forneça credenciais para se conectar ao SnapCenter Server: *Open-SMConnection*
3. Restaure o backup do repositório usando o cmdlet *Restore-SmRepositoryBackup*.

   O cmdlet a seguir restaura o repositório de banco de dados MySQL do SnapCenter a partir dos backups existentes no iSCSI LUN ou no VMDK:

   ```
   C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445
   ```

   O cmdlet a seguir restaura o banco de dados MySQL do SnapCenter quando os arquivos de backup são excluídos acidentalmente no LUN iSCSI. Para o VMDK, restaure manualmente o backup dos snapshots do ONTAP .

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-
x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```

O backup que foi usado para executar a operação de restauração do repositório não será listado quando os backups do repositório forem recuperados após executar a operação de restauração.

Migrar o repositório SnapCenter

Você pode migrar o repositório de banco de dados do SnapCenter Server do local padrão para outro disco. Você pode migrar o repositório quando quiser realocá-lo para um disco com mais espaço.

Passos

1. Pare o serviço MYSQL57 no Windows.
2. Localize o diretório de dados do MySQL.

   Normalmente, você pode encontrar o diretório de dados em C:\ProgramData\MySQL\MySQL Server 5.7\Data.

3. Copie o diretório de dados do MySQL para o novo local, por exemplo, E:\Data\nsm.
4. Clique com o botão direito do mouse no novo diretório e selecione **Propriedades** > **Segurança** para adicionar a conta do servidor local do Serviço de Rede ao novo diretório e, em seguida, atribuir controle total à conta.
5. Renomeie o diretório do banco de dados original, por exemplo, nsm_copy.
6. Em um prompt de comando do Windows, crie um link de diretório simbólico usando o comando *mklink*.

   ```
   "mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
   ```

7. Inicie o serviço MYSQL57 no Windows.
8. Verifique se a alteração do local do banco de dados foi bem-sucedida efetuando login no SnapCenter e verificando as entradas do repositório ou efetuando login no utilitário MySQL e conectando-se ao novo repositório.
9. Exclua o diretório original e renomeado do repositório de banco de dados (nsm_copy).

Redefinir a senha do repositório SnapCenter

A senha do banco de dados do repositório do MySQL Server é gerada automaticamente durante a instalação do SnapCenter Server a partir do SnapCenter 4.2. Essa senha gerada automaticamente não é conhecida pelo usuário do SnapCenter em nenhum momento. Se você quiser acessar o banco de dados do repositório, você deve redefinir a senha.

Antes de começar

Você deve ter privilégios de administrador do SnapCenter para redefinir a senha.

Passos

1. Inicie o PowerShell.

2. No prompt de comando, digite o seguinte comando e forneça as credenciais para se conectar ao SnapCenter Server: *Open-SMConnection*
3. Redefinir a senha do repositório: *Set-SmRepositoryPassword*

   O comando a seguir redefine a senha do repositório:

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: ********
ConfirmPassword: ********
Successfully updated the MySQL server password.
```

Informações relacionadas

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Gerenciar recursos de domínios não confiáveis

Além de gerenciar hosts em domínios confiáveis do Active Directory (AD), o SnapCenter também gerencia hosts em vários domínios não confiáveis do AD. Os domínios do AD não confiáveis devem ser registrados no SnapCenter Server. O SnapCenter oferece suporte a usuários e grupos de vários domínios do AD não confiáveis.

Você pode instalar o SnapCenter Server em uma máquina que esteja em um domínio ou em um grupo de trabalho. Para instalar o SnapCenter Server, você deve especificar as credenciais de domínio se a máquina estiver em um domínio ou as credenciais de administrador local se a máquina estiver em um grupo de trabalho.

Grupos do Active Directory (AD) que pertencem a domínios não registrados no SnapCenter Server não são suportados. Embora você possa criar funções do SnapCenter com esses grupos do AD, o login no SnapCenter Server falha com a seguinte mensagem de erro: O usuário que você está tentando fazer login não pertence a nenhuma função. Entre em contato com seu administrador.

Modificar domínios não confiáveis

Você pode modificar um domínio não confiável quando quiser atualizar os endereços IP do controlador de domínio ou o nome de domínio totalmente qualificado (FQDN).

Sobre esta tarefa

Depois de modificar o FQDN, os ativos associados (hosts, usuários e grupos) podem não funcionar conforme o esperado.

Para modificar um domínio não confiável, você pode usar a interface de usuário do SnapCenter ou cmdlets do PowerShell.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Configurações globais**.
3. Na página Configurações globais, clique em **Configurações de domínio**.
4. Clique  , e então forneça os seguintes detalhes:

Para este campo…	Faça isso…
FQDN de domínio	Especifique o FQDN e clique em **Resolver**.
Endereços IP do controlador de domínio	Se o FQDN do domínio não for resolvível, especifique um ou mais endereços IP do controlador de domínio.

5. Clique em **OK**.

Cancelar registro de domínios não confiáveis do Active Directory

Você pode cancelar o registro de um domínio não confiável do Active Directory se não quiser usar os ativos associados a esse domínio.

Antes de começar

Você deve ter removido os hosts, usuários, grupos e credenciais associados ao domínio não confiável.

Sobre esta tarefa

- Depois que o domínio for cancelado no SnapCenter Server, os usuários desse domínio não poderão acessar o SnapCenter Server.
- Se houver ativos associados (hosts, usuários e grupos), após cancelar o registro do domínio, os ativos não estarão operacionais.
- Para cancelar o registro de um domínio não confiável, você pode usar a interface de usuário do SnapCenter ou os cmdlets do PowerShell.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Configurações globais**.
3. Na página Configurações globais, clique em **Configurações de domínio**.
4. Na lista de domínios, selecione o domínio que você deseja cancelar o registro.
5. Clique e clique em **OK**.

Gerenciar o sistema de armazenamento

Depois de adicionar o sistema de armazenamento, você pode modificar a configuração e as conexões do sistema de armazenamento ou excluí-lo.

Modificar a configuração do sistema de armazenamento

Você pode usar o SnapCenter para modificar a configuração do seu sistema de armazenamento se quiser alterar o nome de usuário, a senha, a plataforma, a porta, o protocolo, o período de tempo limite, o endereço IP preferencial ou as opções de mensagens.

Sobre esta tarefa

Você pode modificar as conexões de armazenamento para um usuário individual ou para um grupo. Se você pertencer a um ou mais grupos com permissão para o mesmo sistema de armazenamento, o nome da conexão de armazenamento será exibido várias vezes na lista de conexões de armazenamento, uma vez para cada grupo com permissão para o sistema de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Sistemas de armazenamento**.
2. Na página Sistemas de Armazenamento, no menu suspenso **Tipo**, execute uma das seguintes ações:

Selecione…	Passos…
SVMs ONTAP	Para visualizar todas as máquinas virtuais de armazenamento (SVMs) que foram adicionadas e modificar a configuração de SVM necessária. a. Na página Conexões de armazenamento, clique no nome do SVM apropriado. b. Execute uma das seguintes ações: ◦ Se o SVM não fizer parte de nenhum cluster, na página Modificar sistema de armazenamento, modifique as configurações, como nome de usuário, senha, configurações de EMS e AutoSupport , plataforma, protocolo, porta, tempo limite e IP preferencial. ◦ Se o SVM fizer parte de um cluster, na página Modificar sistema de armazenamento, selecione **Gerenciar SVM independentemente** e modifique as configurações, como nome de usuário, senha, configurações de EMS e AutoSupport , plataforma, protocolo, porta, tempo limite e IP preferencial. Após modificar o SVM para ser gerenciado de forma independente, se você decidir gerenciá-lo por meio do cluster, exclua o SVM e clique em **Rediscover**. O SVM será adicionado ao cluster ONTAP . Quando uma senha do sistema de armazenamento é atualizada na GUI do SnapCenter , você deve reiniciar os serviços do SMCore do respectivo plug-in ou do host do servidor porque a senha atualizada não é refletida no SMCore, e os trabalhos de backup falharão com um erro de credencial incorreta.

Selecione…	Passos…
Clusters ONTAP	Para visualizar todos os clusters que foram adicionados e modificar a configuração de cluster necessária. a. Na página Conexões de armazenamento, clique no nome do cluster. b. Na página Modificar sistema de armazenamento, clique no ícone de edição ao lado de Nome de usuário e modifique o nome de usuário e a senha. c. Selecione ou desmarque as configurações do EMS e do AutoSupport . d. Clique em **Mais opções** e modifique outras configurações, como plataforma, protocolo, porta, tempo limite e IP preferencial.

3. Clique em **Enviar**.

Excluir o sistema de armazenamento

Você pode usar o SnapCenter para excluir qualquer sistema de armazenamento não utilizado.

Sobre esta tarefa

Você pode excluir conexões de armazenamento para um usuário individual ou para um grupo. Se você pertencer a um ou mais grupos com permissão para o mesmo sistema de armazenamento, o nome do sistema de armazenamento será exibido várias vezes na lista de conexões de armazenamento, uma vez para cada grupo com permissão para o sistema de armazenamento.

Ao excluir um sistema de armazenamento, todas as operações que estão sendo executadas nesse sistema de armazenamento falharão.

Passos

1. No painel de navegação esquerdo, clique em **Sistemas de armazenamento**.
2. Na página Sistemas de Armazenamento, no menu suspenso **Tipo**, selecione * ONTAP SVMs* ou * ONTAP Clusters*.
3. Na página Conexões de armazenamento, marque a caixa de seleção ao lado do SVM ou do cluster que você deseja excluir.

   Você não pode selecionar o SVM que faz parte de um cluster.

4. Clique em **Excluir**.
5. Na página Excluir configurações de conexão do sistema de armazenamento, clique em **OK**.

   Se uma SVM for excluída do cluster ONTAP usando a GUI do ONTAP , na GUI do SnapCenter , clique em **Rediscover** para atualizar a lista de SVMs.

Suporte à API REST

Todas as conexões de sistemas ASA, AFF ou FAS com o ONTAP passarão pelo ZAPI por padrão. A API REST pode ser habilitada para versões específicas do ONTAP .

O SnapCenter utiliza APIs REST para executar todas as operações em sistemas ASA r2, que não oferecem suporte a ZAPIs.

Você pode modificar as chaves de configuração nos seguintes arquivos de configuração:

- IsRestEnabledForStorageConnection

  O valor padrão é falso.

- Versão MinOntap para usar REST

  O valor padrão é 9.13.1.

Habilitar conexão por meio da API REST

1. Defina IsRestEnabledForStorageConnection como verdadeiro.
2. Adicione a chave em SMCoreServiceHost.dll.config e SnapDriveService.dll.config nos hosts do servidor e do plug-in do Windows.

   <adicionar chave="IsRestEnabledForStorageConnection" valor="true" />

Limitar a conexão por meio da API REST a uma versão específica do ONTAP

1. Defina o parâmetro de configuração MinOntapVersionToUseREST como verdadeiro.
2. Adicione a chave em SMCoreServiceHost.dll.config e SnapDriveService.dll.config nos hosts do servidor e do plug-in do Windows.

   <adicionar chave="MinOntapVersionToUseREST" valor="9.13.1" />

3. Reinicie o serviço do SmCore no servidor e o serviço do plug-in e do SnapDrive na máquina do plug-in.

Gerenciar coleta de dados de EMS

Você pode agendar e gerenciar a coleta de dados do Sistema de Gerenciamento de Eventos (EMS) usando cmdlets do PowerShell. A coleta de dados do EMS envolve a coleta de detalhes sobre o SnapCenter Server, os pacotes de plug-in SnapCenter instalados, os hosts e informações semelhantes e, em seguida, o envio para uma máquina virtual de armazenamento ONTAP (SVM) especificada.

> A utilização da CPU do sistema é alta quando a tarefa de coleta de dados está em andamento. A utilização da CPU permanece alta enquanto a operação progride, independentemente do tamanho dos dados.

Interrompa a coleta de dados do EMS

A coleta de dados do EMS é ativada por padrão e é executada a cada sete dias após a data de instalação. Você pode desabilitar a coleta de dados a qualquer momento usando o cmdlet do PowerShell *Disable-*

SmDataCollectionEMS.

Passos

1. Em uma linha de comando do PowerShell, estabeleça uma sessão com o SnapCenter digitando *Open-SmConnection*.
2. Desabilite a coleta de dados do EMS digitando *Disable-SmDataCollectionEms*.

Iniciar coleta de dados do EMS

A coleta de dados do EMS é habilitada por padrão e está programada para ser executada a cada sete dias a partir da data de instalação. Se você o desativou, poderá iniciar a coleta de dados do EMS novamente usando o cmdlet *Enable-SmDataCollectionEMS*.

A permissão generate-autosupport-log do evento NetApp ONTAP foi concedida ao usuário da máquina virtual de armazenamento (SVM).

Passos

1. Em uma linha de comando do PowerShell, estabeleça uma sessão com o SnapCenter digitando *Open-SmConnection*.
2. Habilite a coleta de dados do EMS inserindo *Enable-SmDataCollectionEMS*.

Alterar cronograma de coleta de dados do EMS e SVM de destino

Você pode usar cmdlets do PowerShell para alterar o cronograma de coleta de dados do EMS ou a máquina virtual de armazenamento de destino (SVM).

Passos

1. Em uma linha de comando do PowerShell, para estabelecer uma sessão com o SnapCenter, insira o cmdlet *Open-SmConnection*.
2. Para alterar o destino da coleta de dados do EMS, insira o cmdlet *Set-SmDataCollectionEmsTarget*.
3. Para alterar o cronograma de coleta de dados do EMS, insira o cmdlet *Set-SmDataCollectionEmsSchedule*.

Monitorar o status da coleta de dados do EMS

Você pode monitorar o status da coleta de dados do EMS usando vários cmdlets do PowerShell. Você pode obter informações sobre o cronograma, o destino da máquina virtual de armazenamento (SVM) e o status.

Passos

1. Em uma linha de comando do PowerShell, estabeleça uma sessão com o SnapCenter digitando *Open-SmConnection*.
2. Recupere informações sobre o cronograma de coleta de dados do EMS inserindo *Get-SmDataCollectionEmsSchedule*.
3. Recupere informações sobre o status da coleta de dados do EMS inserindo *Get-SmDataCollectionEmsStatus*.
4. Recupere informações sobre o alvo de coleta de dados do EMS inserindo *Get-SmDataCollectionEmsTarget*.

Informações relacionadas

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser

obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Atualizar o SnapCenter Server e os plug-ins

Configure o SnapCenter para verificar se há atualizações disponíveis

O SnapCenter se comunica periodicamente com o site de suporte da NetApp para notificá-lo sobre atualizações de software disponíveis. Você também pode criar uma programação para especificar o intervalo em que deseja receber informações sobre atualizações disponíveis.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página **Configurações**, clique em **Software**.

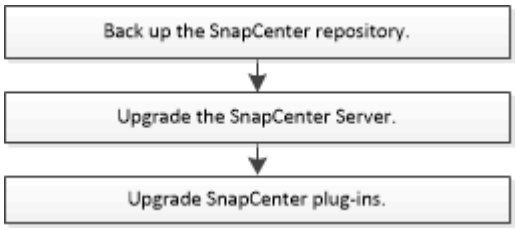
   A página Software disponível exibe os pacotes de plug-ins disponíveis, as versões disponíveis e seu status de instalação.

3. Clique em **Verificar atualizações** para ver se há versões mais recentes de pacotes de plug-ins disponíveis.
4. Clique em **Agendar atualizações** para criar uma programação para especificar o intervalo em que você deseja receber informações sobre atualizações disponíveis:
   a. Selecione o intervalo em **Verificar atualizações**.
   b. Selecione a credencial do SnapCenter Server Admin Windows e clique em **OK**.

Fluxo de trabalho de atualização

Cada versão do SnapCenter contém um SnapCenter Server atualizado e um pacote de plug-in. As atualizações do pacote de plug-in são distribuídas com o instalador do SnapCenter . Você pode configurar o SnapCenter para verificar se há atualizações disponíveis.

O fluxo de trabalho mostra as diferentes tarefas necessárias para atualizar o SnapCenter Server e os pacotes de plug-in.



Caminhos de atualização suportados

O caminho de atualização ajuda você a entender quais versões anteriores do SnapCenter você pode atualizar para as versões mais recentes do SnapCenter e quais versões dos plug-ins são suportadas.

Se você estiver na versão SnapCenter Server…	Você pode atualizar diretamente o SnapCenter Server para…	Versões de plug-in suportadas
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

Para obter informações sobre como atualizar o SnapCenter Plug-in for VMware vSphere, consulte "Atualizar o SnapCenter Plug-in for VMware vSphere" .

Atualizar o SnapCenter Server no host Windows

Você deve atualizar o SnapCenter Server para acessar os recursos e aprimoramentos mais recentes fornecidos na versão mais recente.

Antes de começar

- Atualize o host do SnapCenter Server com as atualizações mais recentes do Windows e certifique-se de que não haja reinicializações pendentes do sistema.
- Certifique-se de que nenhuma outra operação esteja em execução antes de iniciar a atualização.
- Instale o ASP.NET Core Runtime 8.0.12 (e todos os patches 8.0.x subsequentes), o Hosting Bundle e o PowerShell 7.4.2 ou posterior.
- Faça backup do banco de dados do repositório SnapCenter (MySQL) depois de garantir que nenhuma tarefa esteja em execução. Isso é recomendado antes de atualizar o SnapCenter Server e o plug-in do Exchange.

  Para obter informações, consulte"Faça backup do repositório SnapCenter" .

- Faça backup de todos os arquivos de configuração do SnapCenter modificados no host do SnapCenter Server ou no host do plug-in.

  Exemplos de arquivos de configuração do SnapCenter : SnapDriveService.exe.config, SMCoreServiceHost.exe.config e assim por diante.

- Se você instalou várias versões do plug-in personalizado no SnapCenter 5.0, antes de atualizar para a versão 6.0 ou posterior, execute os cmdlets do PowerShell para remover todas as versões anteriores do plug-in personalizado (exceto a mais recente) do repositório do SnapCenter (banco de dados NSM).

- Correr `Open-SmConnection` e faça login usando as credenciais da função SnapCenterAdmin
- Correr `Remove-SmPluginPackage -PluginName M<plug-in name> -PluginVersion <version number>`

  Para obter mais informações, consulte "Falha na atualização para o SnapCenter 6.0 ou posterior" .

Sobre esta tarefa

- Durante a atualização, o SnapCenter executa um script SQL para atualizar os dados do Exchange no banco de dados NSM, convertendo o DAG e o nome abreviado do host em FQDN. Isso se aplica somente se você usar o SnapCenter Server com o plug-in do Exchange.
- Se você colocou manualmente o host do servidor no modo de manutenção, após a atualização selecione **Hosts** > **Ativar agendamento** para tirar o host do servidor do modo de manutenção.
- Para os agendamentos de backup e verificação existentes com prescrições e pós-escritos habilitados na política, as operações de backup continuarão a funcionar após a atualização.

  Na página **Detalhes do trabalho**, uma mensagem de aviso recomenda que o cliente copie os scripts para o SCRIPTS_PATH e edite a política para fornecer um caminho relativo ao SCRIPTS_PATH. Para o trabalho do ciclo de vida do clone, a mensagem de aviso aparece no nível do subtrabalho.

Passos

1. Baixe o pacote de instalação do SnapCenter Server no site de suporte da NetApp .

   https://mysupport.netapp.com/site/products/all/details/snapcenter/downloads-tab

2. Crie uma cópia do web.config localizado em C:\Program Files\ NetApp\ SnapCenter WebApp.
3. Exporte os agendamentos do host do plug-in SnapCenter do Agendador de Tarefas do Windows para restaurá-los se a atualização falhar.

   ```
   md d:\\SCBackup``schtasks /query /xml /TN taskname >>
   "D:\SCBackup\taskname.xml"
   ```

4. Crie o dump do banco de dados MySQL do SnapCenter se o backup do repositório não estiver configurado.

   ```
   md d:\\SCBackup``mysqldump --all-databases --single-transaction --add-drop
   -database --triggers --routines --events -u root -p >
   D:\SCBackup\SCRepoBackup.dmp
   ```

   Quando solicitado, digite a senha.

5. Clique duas vezes no arquivo .exe baixado para iniciar a atualização do SnapCenter Server.

   Depois de iniciar a atualização, o SnapCenter executa pré-verificações. Se o sistema não atender aos requisitos mínimos, o SnapCenter mostrará mensagens de erro ou aviso. Você pode ignorar os avisos e continuar com a instalação, mas deve corrigir quaisquer erros.

   > O SnapCenter continua a usar a senha do banco de dados do repositório MySQL Server existente fornecida durante a instalação da versão anterior do SnapCenter Server.

6. Selecione **Atualizar**.

Se você selecionar **Cancelar** em qualquer estágio, o SnapCenter interromperá a atualização. Ele não reverterá o SnapCenter Server para o estado anterior.

Melhores práticas: Saia e faça login novamente ou abra um novo navegador para acessar a interface do usuário do SnapCenter .

Depois que você terminar

- Se o plug-in for instalado usando um usuário sudo, você deverá copiar as chaves sha224 disponíveis em *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* para atualizar o arquivo */etc/sudoers*.
- Você deve realizar uma nova descoberta de recursos no host do servidor.

  Se o SnapCenter exibir o status do host do servidor como parado, aguarde um pouco e execute uma nova descoberta. Você também pode alterar o valor do parâmetro **HostRefreshInterval** (o valor padrão é 3600 segundos) para qualquer valor maior que 10 minutos.

- Se a atualização falhar, limpe a instalação com falha, reinstale a versão anterior do SnapCenter e restaure o banco de dados NSM para o estado em que estava antes.
- Após atualizar o host do servidor, você também deve atualizar os plug-ins antes de adicionar qualquer sistema de armazenamento.

Atualizar o SnapCenter Server no host Linux

Você pode usar o arquivo do instalador do SnapCenter Server para atualizar o SnapCenter Server.

Passos

1. Execute uma das ações para atualizar o SnapCenter Server.

Se você quiser executar…	Faça isso…
Atualização não interativa	`sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DUPGRADE=<value> -DINSTALL_LOG_NAME=<filename>` Exemplo: sudo ./snapcenter_linux_server.bin -i silent -DUPGRADE=1 -DINSTALL_LOG_NAME=InstallerLog.log Os logs serão armazenados em */var/opt/snapcenter/logs*. Parâmetros a serem passados para atualização: • DINSTALL_LOG_NAME: Nome do arquivo de log onde os logs de instalação serão armazenados. • DUPGRADE: O valor padrão é 0. Especifique este parâmetro e seu valor como qualquer número inteiro diferente de 0 para atualizar o SnapCenter Server.
Instalação interativa	`./snapcenter-linux-server-(el8/el9/sles15).bin` Você será solicitado a confirmar a atualização. Insira qualquer valor diferente de 0 para confirmar a atualização do SnapCenter Server.

Você deve sair e depois entrar no SnapCenter ou fechar e abrir um novo navegador para acessar a interface gráfica do usuário do SnapCenter .

Atualize seus pacotes de plug-ins

Os pacotes de plug-in são distribuídos como parte da atualização do SnapCenter .

Você não precisa colocar manualmente cada host de plug-in que deseja atualizar no modo de manutenção porque o procedimento de atualização coloca seus hosts de plug-in Windows, Linux ou AIX no modo de manutenção. O modo de manutenção impede que quaisquer tarefas agendadas sejam executadas no host do plug-in durante a atualização.

Antes de começar

- Se você for um usuário não root com acesso às máquinas Linux, atualize o arquivo */etc/sudoers* com os valores de soma de verificação mais recentes antes de executar a operação de atualização.
- Por padrão, o SnapCenter detecta JAVA_HOME do ambiente. Se você quiser usar um JAVA_HOME fixo e estiver atualizando os plug-ins em um host Linux, adicione manualmente o parâmetro SKIP_JAVAHOME_UPDATE no arquivo *spl.properties* localizado em */var/opt/snapcenter/spl/etc/* e defina o valor como TRUE.

O valor de JAVA_HOME é atualizado quando o plug-in é atualizado ou quando o serviço do carregador de plug-in do SnapCenter (SPL) é reiniciado. Antes de atualizar ou reiniciar o SPL, se você adicionar o parâmetro SKIP_JAVAHOME_UPDATE e definir o valor como TRUE, o valor de JAVA_HOME não será atualizado.

- Você deve ter feito backup de todos os arquivos de configuração do SnapCenter que você modificou no host do SnapCenter Server ou no host do plug-in.

  Exemplos de arquivos de configuração do SnapCenter : SnapDriveService.exe.config, SMCoreServiceHost.exe.config e assim por diante.

Sobre esta tarefa

- Para o SnapCenter Plug-in para Microsoft SQL Server, SnapCenter Plug-in para Microsoft Exchange Server e SnapCenter Plug-in para Microsoft Windows, é recomendável atualizar o servidor e os hosts do plug-in para a versão mais recente para que o SCRIPTS_PATH seja executado.

  Para os agendamentos de backup e verificação existentes com prescrições e pós-escritos habilitados na política, as operações de backup continuarão a funcionar após a atualização.

  Na página **Detalhes do trabalho**, uma mensagem de aviso recomenda que o cliente copie os scripts para o SCRIPTS_PATH e edite a política para fornecer um caminho relativo ao SCRIPTS_PATH. Para o trabalho do ciclo de vida do clone, a mensagem de aviso aparece no nível do subtrabalho.

Passos

1. No painel de navegação esquerdo, clique em **Hosts** > **Hosts gerenciados**.
2. Atualize os hosts executando uma das seguintes tarefas:

   - Se a coluna Status geral exibir "Atualização disponível" para um dos hosts de plug-in, clique no nome do host do plug-in e execute o seguinte:
     i. Clique em **Mais opções**.
     ii. Selecione **Ignorar pré-verificações** se não quiser validar se o host do plug-in atende aos requisitos para atualizar o plug-in.
     iii. Clique em **Atualizar**.
   - Se você deseja atualizar vários hosts, selecione todos os hosts, clique em e clique em **Atualizar** > **OK**.

     Todos os serviços relacionados são reiniciados durante a atualização do plug-in.

     Todos os plug-ins no pacote são selecionados, mas somente os plug-ins que foram instalados com a versão anterior do SnapCenter são atualizados, e os plug-ins restantes não são instalados. Você deve usar a opção **Adicionar plug-ins** para instalar qualquer novo plug-in.

     Se você não tiver marcado a caixa de seleção **Ignorar pré-verificações**, o host do plug-in será validado para verificar se atende aos requisitos para a instalação do plug-in. Se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas serão exibidas. Após corrigir o problema, clique em **Atualizar**.

Se o erro estiver relacionado ao espaço em disco ou à RAM, você poderá atualizar o web.config localizado em C:\Program Files\ NetApp\ SnapCenter WebApp ou os arquivos de configuração do PowerShell localizados em C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ SnapCenter\ para modificar os valores padrão. Se o erro estiver relacionado aos parâmetros restantes, você deverá corrigir o problema e validar os requisitos novamente.

Atualização tecnológica

Atualização tecnológica do host do SnapCenter Server

Quando o host do SnapCenter Server precisar ser atualizado, você poderá instalar a mesma versão do SnapCenter Server no novo host e, em seguida, executar as APIs para fazer backup do SnapCenter do servidor antigo e restaurá-lo no novo servidor.

Passos

1. Implante o novo host e execute as seguintes tarefas:
   a. Instale a mesma versão do SnapCenter Server.
   b. (Opcional) Configure certificados de CA e habilite SSL bidirecional. Para mais informações, consulte "Configurar certificado CA" e "Configurar e habilitar SSL bidirecional" .
   c. (Opcional) Configure a autenticação multifator. Para obter mais informações, consulte "Habilitar autenticação multifator" .
2. Efetue login como usuário administrador do SnapCenter .
3. Crie um backup do SnapCenter Server no host antigo usando a API: `/<snapcenter_version>/server/backup` ou o cmdlet: *New-SmServerBackup*.

   Antes de fazer o backup, suspenda todos os trabalhos agendados e certifique-se de que nenhum trabalho esteja em execução.

   Se você quiser restaurar o backup no SnapCenter Server que está sendo executado em um novo domínio, antes de fazer um backup, você deve adicionar o novo usuário de domínio no antigo host SnapCenter e atribuir a função de administrador do SnapCenter .

4. Copie o backup do host antigo para o novo.
5. Restaure o backup do SnapCenter Server no novo host usando a API: `/<snapcenter_version>/server/restore` ou o cmdlet: *Restore-SmServerBackup*.

   A restauração atualizará o novo URL do SnapCenter Server em todos os hosts por padrão. Se você quiser pular a atualização, use o atributo *-SkipSMSURLInHosts* e atualize separadamente a URL do servidor executando usando a API: `/<snapcenter_version>/server/configureurl` ou o cmdlet: *Set-SmServerConfig*.

   Se o host do plug-in não conseguir resolver o nome do host do servidor, faça login em cada host do plug-in e adicione a entrada *etc/host* para o novo IP no formato <Novo IP> SC_Server_Name.

   As entradas do servidor *etc/host* não serão restauradas. Você pode restaurá-lo manualmente a partir do servidor antigo.

   Se o backup for restaurado no SnapCenter Server que está sendo executado em um novo domínio e você quiser continuar a usar os usuários do domínio antigo, registre o domínio antigo no novo SnapCenter Server.

Se você tiver atualizado manualmente o arquivo web.config no host antigo do SnapCenter , as atualizações não serão copiadas para o novo host. Você deve fazer manualmente as mesmas alterações no arquivo web.config do novo host.

6. Se você pulou a atualização do URL do SnapCenter Server ou se algum host ficou inativo durante o processo de restauração, atualize o novo nome do servidor em todos os hosts ou hosts especificados que são gerenciados pelo SnapCenter usando a API: `/<snapcenter_version>/server/configureurl` ou o cmdlet: *Set-SmServerConfig*.
7. Ative os trabalhos agendados em todos os hosts do novo SnapCenter Server.

Atualização tecnológica de um nó no cluster F5

Você pode fazer uma atualização técnica de qualquer nó no cluster F5 removendo o nó e adicionando o novo nó. Se o nó que precisa ser atualizado estiver ativo, torne outro nó do cluster ativo e remova-o.

Para obter informações sobre como adicionar um nó ao cluster F5, consulte "Configurar servidores SnapCenter para alta disponibilidade usando F5" .

Se a URL do cluster F5 mudar, ela poderá ser atualizada em todos os hosts usando a API: `/<snapcenter_version>/server/configureurl` ou o cmdlet: *Set-SmServerConfig*.

Desativando o antigo host do SnapCenter Server

Você pode remover o antigo host do SnapCenter Server após verificar se o novo SnapCenter Server está ativo e em execução e se todos os hosts de plug-in conseguem se comunicar com o novo host do SnapCenter Server.

Reverter para o antigo host do SnapCenter Server

Em caso de problemas, você pode trazer de volta o antigo host do SnapCenter Server atualizando a URL do SnapCenter Server em todos os hosts usando a API: `/<snapcenter_version>/server/configureurl` ou o cmdlet: *Set-SmServerConfig*.

Recuperação de desastres

Recuperação de desastres do host SnapCenter autônomo

Você pode executar a recuperação de desastres restaurando o backup do servidor para o novo host.

Antes de começar

Certifique-se de ter um backup do antigo SnapCenter Server.

Passos

1. Implante o novo host e execute as seguintes tarefas:
   a. Instale a mesma versão do SnapCenter Server.
   b. Configure certificados de CA e habilite SSL bidirecional. Para mais informações, consulte "Configurar certificado CA" e "Configurar e habilitar SSL bidirecional" .
2. Copie o backup antigo do SnapCenter Server para o novo host.
3. Efetue login como usuário administrador do SnapCenter .

4. Restaure o backup do SnapCenter Server no novo host usando a API: `/<snapcenter_version>/server/restore` ou o cmdlet: *Restore-SmServerBackup*.

   A restauração atualizará o novo URL do SnapCenter Server em todos os hosts por padrão. Se você quiser pular a atualização, use o atributo *-SkipSMSURLInHosts* e atualize separadamente a URL do servidor usando a API: `/<snapcenter_version>/server/configureurl` ou o cmdlet: *Set-SmServerConfig*.

   Se o host do plug-in não conseguir resolver o nome do host do servidor, faça login em cada host do plug-in e adicione a entrada *etc/host* para o novo IP no formato <Novo IP> SC_Server_Name.

   As entradas do servidor *etc/host* não serão restauradas. Você pode restaurá-lo manualmente a partir do servidor antigo.

5. Se você pulou a atualização da URL ou algum host ficou inativo durante o processo de restauração, atualize o novo nome do servidor em todos os hosts ou hosts especificados que são gerenciados pelo SnapCenter usando a API: `/<snapcenter_version>/server/configureurl` ou o cmdlet: *Set-SmServerConfig*.

Recuperação de desastres do cluster SnapCenter F5

Você pode executar a recuperação de desastres restaurando o backup do servidor para o novo host e, em seguida, convertendo o host autônomo em um cluster.

Antes de começar

Certifique-se de ter um backup do antigo SnapCenter Server.

Passos

1. Implante o novo host e execute as seguintes tarefas:
   a. Instale a mesma versão do SnapCenter Server.
   b. Configure certificados de CA e habilite SSL bidirecional. Para mais informações, consulte "Configurar certificado CA" e "Configurar e habilitar SSL bidirecional" .
2. Copie o backup antigo do SnapCenter Server para o novo host.
3. Efetue login como usuário administrador do SnapCenter .
4. Restaure o backup do SnapCenter Server no novo host usando a API: `/<snapcenter_version>/server/restore` ou o cmdlet: *Restore-SmServerBackup*.

   A restauração atualizará o novo URL do SnapCenter Server em todos os hosts por padrão. Se você quiser pular a atualização, use o atributo *-SkipSMSURLInHosts* e atualize separadamente a URL do servidor usando a API: `/<snapcenter_version>/server/configureurl` ou o cmdlet: *Set-SmServerConfig*.

   Se o host do plug-in não conseguir resolver o nome do host do servidor, faça login em cada host do plug-in e adicione a entrada *etc/host* para o novo IP no formato <Novo IP> SC_Server_Name.

   As entradas do servidor *etc/host* não serão restauradas. Você pode restaurá-lo manualmente a partir do servidor antigo.

5. Se você pulou a atualização da URL ou algum host ficou inativo durante o processo de restauração,

atualize o novo nome do servidor em todos os hosts ou hosts especificados que são gerenciados pelo SnapCenter usando a API: `/<snapcenter_version>/server/configureurl` ou o cmdlet: *Set-SmServerConfig*.

6. Converta o host autônomo em cluster F5.

   Para obter informações sobre como configurar o F5, consulte "Configurar servidores SnapCenter para alta disponibilidade usando F5" .

Informações relacionadas

Para obter informações sobre as APIs, você precisa acessar a página do Swagger. veja"Como acessar APIs REST usando a página da web da API do Swagger" .

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Atualização tecnológica dos hosts de plug-in SnapCenter

Quando os hosts do plug-in SnapCenter precisarem ser atualizados, você deverá mover os recursos do host antigo para o novo. Quando o novo host for adicionado ao SnapCenter, ele descobrirá todos os recursos, mas será tratado como novos recursos.

Sobre esta tarefa

Você deve executar a API ou o cmdlet que usará o nome do host antigo e o nome do novo host como entrada, comparará os recursos por nome e vinculará novamente os objetos de recursos correspondentes do host antigo ao novo. Os recursos correspondentes serão marcados como protegidos.

- O parâmetro *IsDryRun* é definido como True por padrão e isso identifica os recursos correspondentes do host antigo e do novo.

  Após verificar os recursos correspondentes, você deve definir o parâmetro *IsDryRun* como False para revincular os objetos dos recursos correspondentes do host antigo para o novo host.

- O parâmetro *AutoMigrateManuallyAddedResources* é definido como True por padrão e isso copia automaticamente os recursos adicionados manualmente do host antigo para o novo host.

  O parâmetro *AutoMigrateManuallyAddedResources* é aplicável somente aos recursos Oracle e SAP HANA.

- O parâmetro *SQLInstanceMapping* deve ser usado se o nome da instância for diferente entre o host antigo e o novo. Se for uma instância padrão, use *default_instance* como nome da instância.

A atualização de tecnologia é compatível com os seguintes plug-ins do SnapCenter :

- Plug-in SnapCenter para Microsoft SQL Server
  - Se os bancos de dados SQL forem protegidos no nível da instância e, como parte da atualização tecnológica do host, apenas recursos parciais forem movidos para o novo host, a proteção existente no nível da instância será convertida em proteção do grupo de recursos e as instâncias de ambos os hosts serão adicionadas ao grupo de recursos.
  - Se um host SQL (por exemplo, host1) for usado como agendador ou servidor de verificação para recursos de outro host (por exemplo, host2), ao executar a atualização de tecnologia no host1, o agendamento ou os detalhes de verificação não serão migrados e continuarão a ser executados no

host1. Se você precisar modificar, deverá fazer isso manualmente nos respectivos hosts.

  - Se estiver usando a configuração de SQL Failover Cluster Instances (FCI), você poderá executar a atualização técnica adicionando o novo nó ao cluster FCI e atualizando o host do plug-in no SnapCenter.
  - Se você estiver usando a configuração do SQL Availability Group (AG), a atualização tecnológica não será necessária. Você pode adicionar o novo nó ao AG e atualizar o host no SnapCenter.

- Plug-in SnapCenter para Windows
- Plug-in SnapCenter para banco de dados Oracle

  Se estiver usando a configuração do Oracle Real Application Cluster (RAC), você poderá executar a atualização técnica adicionando o novo nó ao cluster RAC e atualizando o host do plug-in no SnapCenter.

- Plug-in SnapCenter para banco de dados SAP HANA

Os casos de uso suportados são:

- Migrando recursos de um host para outro.
- Migração de recursos de vários hosts para um ou menos hosts.
- Migrando recursos de um host para vários hosts.

Os cenários suportados são:

- O novo host tem um nome diferente do antigo host
- O host existente foi renomeado

Antes de começar

Como esse fluxo de trabalho modifica os dados no repositório do SnapCenter , é recomendável fazer backup do repositório do SnapCenter . Em caso de problemas com os dados, o repositório SnapCenter pode ser revertido para o estado antigo usando o backup.

Para obter mais informações, consulte "Faça backup do repositório SnapCenter" .

Passos

1. Implante o novo host e instale o aplicativo.
2. Suspenda as programações do antigo host.
3. Mova os recursos necessários do host antigo para o novo host.
   a. Abra os bancos de dados necessários no novo host a partir do mesmo armazenamento.
      - Certifique-se de que o armazenamento esteja mapeado para a mesma unidade ou mesmo caminho de montagem do host antigo. Se o armazenamento não estiver mapeado corretamente, os backups criados no host antigo não poderão ser usados para restauração.

        Por padrão, o Windows atribui automaticamente a próxima unidade disponível.

      - Se o DR de armazenamento estiver habilitado, o respectivo armazenamento deverá ser montado no novo host.
   b. Verifique a compatibilidade caso haja alguma alteração na versão do aplicativo.
   c. Somente para o host do plug-in Oracle, certifique-se de que os UIDs e GIDs do Oracle e seus usuários de grupo sejam os mesmos do host antigo.

Para obter informações, consulte:

- "Como migrar o banco de dados SQL do host antigo para o novo"
- "Como migrar o banco de dados Oracle do host antigo para o novo"
- "Como instalar o banco de dados SAP HANA em um novo host"

4. Adicione o novo host ao SnapCenter.
5. Verifique se todos os recursos foram descobertos.
6. Execute a API de atualização do host: `/<snapcenter_version>/techrefresh/host` ou o cmdlet: *Invoke-SmTechRefreshHost*.

   A execução de teste é ativada por padrão e os recursos correspondentes a serem revinculados são identificados. Você pode verificar os recursos executando a API: '/jobs/{jobid}' ou o cmdlet *Get-SmJobSummaryReport*.

   Se você tiver migrado os recursos de vários hosts, deverá executar a API ou o cmdlet para todos os hosts. Se a unidade ou o caminho de montagem no novo host não for o mesmo do host antigo, as seguintes operações de restauração falharão:

   - A restauração local do SQL falhará. No entanto, o recurso RTAL pode ser aproveitado.
   - A restauração dos bancos de dados Oracle e SAP HANA falhará.

   Se você quiser migrar para vários hosts, execute todas as etapas do passo 1 para todos os hosts.

   Você pode executar a API ou o cmdlet no mesmo host várias vezes; ele só será vinculado novamente se um novo recurso for identificado.

7. (Opcional) Remova o host ou hosts antigos do SnapCenter.

Informações relacionadas

Para obter informações sobre as APIs, você precisa acessar a página do Swagger. veja"Como acessar APIs REST usando a página da web da API do Swagger" .

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Atualização tecnológica do sistema de armazenamento

Quando o armazenamento é atualizado tecnicamente, os dados são migrados para o novo armazenamento e os hosts do aplicativo são montados com o novo armazenamento. O fluxo de trabalho de backup do SnapCenter identifica o novo armazenamento e cria o instantâneo se o novo armazenamento estiver registrado no SnapCenter.

Você pode executar restauração, montagem e clonagem nos novos backups criados após a atualização do armazenamento. No entanto, essas operações falharão quando executadas em backups criados antes da atualização do armazenamento porque os backups têm os detalhes de armazenamento antigos. Você deve executar a API ou o cmdlet de atualização de tecnologia de armazenamento para atualizar os backups antigos no SnapCenter com os novos detalhes de armazenamento.

A atualização de tecnologia é compatível com os seguintes plug-ins do SnapCenter :

- Plug-in SnapCenter para Microsoft SQL Server
- Plug-in SnapCenter para Windows
- Plug-in SnapCenter para banco de dados Oracle
- Plug-in SnapCenter para banco de dados SAP HANA
- Plug-in SnapCenter para Microsoft Exchange Server

Os casos de uso suportados são:

- Atualização do armazenamento primário

  A atualização da tecnologia de armazenamento é compatível com a substituição do armazenamento primário por um novo armazenamento. Não é possível converter o armazenamento secundário existente em armazenamento primário.

- Atualização de armazenamento secundário

Atualizar os backups do armazenamento primário

Quando o armazenamento for atualizado tecnicamente, você deverá executar a API ou o cmdlet de atualização tecnológica de armazenamento para atualizar os backups antigos no SnapCenter com os novos detalhes de armazenamento.

Antes de começar

Como esse fluxo de trabalho modifica os dados no repositório do SnapCenter , é recomendável fazer backup do repositório do SnapCenter . Em caso de problemas com os dados, o repositório SnapCenter pode ser revertido para o estado antigo usando o backup.

Para obter mais informações, consulte "Faça backup do repositório SnapCenter" .

Passos

1. Migre os dados do armazenamento antigo para o novo.

   Para obter informações sobre como migrar, consulte:

   - "Como migrar os dados para um novo armazenamento"
   - "Como posso copiar um volume e preservar todas as cópias do Snapshot?"
2. Coloque o host em modo de manutenção.
3. Monte o novo armazenamento nos respectivos hosts e abra os bancos de dados.

   O novo armazenamento deve ser conectado ao host da mesma forma que antes. Por exemplo, se ele foi conectado como SAN, ele precisa ser conectado como SAN.

   O novo armazenamento precisa ser montado na mesma unidade ou caminho do armazenamento antigo.

4. Verifique se todos os recursos estão ativos e funcionando.
5. Adicione o novo armazenamento no SnapCenter.

   Certifique-se de ter um nome SVM exclusivo em todos os clusters no SnapCenter. Se você estiver usando o mesmo nome de SVM no novo armazenamento e se todos os volumes do SVM puderem ser migrados

antes de executar a atualização do armazenamento, é recomendável excluir o SVM no cluster antigo e redescobrir o cluster antigo no SnapCenter , o que removerá o SVM do cache.

6. Coloque o host no modo de produção.
7. No SnapCenter, crie um backup dos recursos cujo armazenamento é migrado. Um novo backup é necessário para que o SnapCenter identifique a pegada de armazenamento mais recente e será usado para atualizar os metadados de backups antigos existentes.

   Sempre que um novo LUN for anexado ao host, ele terá um novo número de série. Durante a descoberta do Sistema de Arquivos do Windows, o SnapCenter tratará cada número de série exclusivo como um novo recurso. Durante a atualização da tecnologia de armazenamento, quando o LUN do novo armazenamento é anexado ao host com a mesma letra de unidade ou caminho, a descoberta do Sistema de Arquivos do Windows no SnapCenter marcará o recurso existente como excluído, mesmo que ele esteja montado com a mesma letra de unidade ou caminho, e exibirá o novo LUN como novo recurso. Como o recurso é marcado como excluído, ele não será considerado para atualização de tecnologia de armazenamento no SnapCenter e todos os backups do recurso antigo serão perdidos. Sempre que ocorrer uma atualização de armazenamento para recursos do sistema de arquivos do Windows, a descoberta de recursos não deve ser realizada antes de executar a API ou o cmdlet de atualização de armazenamento.

8. Execute a API de atualização de armazenamento: `/<snapcenter_version>/techrefresh/primarystorage` ou o cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.

   Se o recurso estiver configurado com uma política de replicação habilitada, o backup mais recente após a atualização do armazenamento deverá ter detalhes do armazenamento secundário.

   a. Se você estiver usando a configuração de SQL Failover Cluster Instances (FCI), os backups serão mantidos no nível do cluster. Você deve fornecer o nome do cluster como entrada para atualização da tecnologia de armazenamento.
   b. Se você estiver usando a configuração do Grupo de Disponibilidade (AG) do SQL, os backups serão mantidos no nível do nó. Você deve fornecer o nome do nó como entrada para atualização de tecnologia de armazenamento.
   c. Se estiver usando a configuração do Oracle Real Application Clusters (RAC), você poderá executar a atualização da tecnologia de armazenamento em qualquer nó.

      O atributo *IsDryRun* é definido como True por padrão. Ele identificará os recursos para os quais o armazenamento será atualizado. Você pode visualizar o recurso e os detalhes de armazenamento alterados executando a API: '<snapcenter_version>/jobs/{jobid}' ou o cmdlet *Get-SmJobSummaryReport*.

9. Depois de verificar os detalhes do armazenamento, defina o atributo *IsDryRun* como False e execute a API de atualização de armazenamento: `/<snapcenter_version>/techrefresh/primarystorage` ou o cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.

   Isso atualizará os detalhes de armazenamento nos backups mais antigos.

   Você pode executar a API ou o cmdlet no mesmo host várias vezes. Ele atualizará os detalhes de armazenamento nos backups mais antigos somente se o armazenamento for atualizado.

A hierarquia de clones não pode ser migrada no ONTAP. Se o armazenamento que está sendo migrado tiver metadados clonados no SnapCenter, o recurso clonado será marcado como recurso independente. Clones de metadados de clones serão removidos recursivamente.

10. (Opcional) Se todos os snapshots não forem movidos do armazenamento primário antigo para o novo, execute a seguinte API: `/<snapcenter_version>/hosts/primarybackupsexistencecheck` ou o cmdlet *Invoke-SmPrimaryBackupsExistenceCheck*.

    Isso executará a verificação de existência do snapshot no novo armazenamento primário e marcará os respectivos backups como não disponíveis para nenhuma operação no SnapCenter.

Atualizar os backups do armazenamento secundário

Quando o armazenamento for atualizado tecnicamente, você deverá executar a API ou o cmdlet de atualização tecnológica de armazenamento para atualizar os backups antigos no SnapCenter com os novos detalhes de armazenamento.

Antes de começar

Como esse fluxo de trabalho modifica os dados no repositório do SnapCenter , é recomendável fazer backup do repositório do SnapCenter . Em caso de problemas com os dados, o repositório SnapCenter pode ser revertido para o estado antigo usando o backup.

Para obter mais informações, consulte "Faça backup do repositório SnapCenter" .

Passos

1. Migre os dados do armazenamento antigo para o novo.

   Para obter informações sobre como migrar, consulte:

   - "Como migrar os dados para um novo armazenamento"
   - "Como posso copiar um volume e preservar todas as cópias do Snapshot?"
2. Estabeleça o relacionamento SnapMirror entre o armazenamento primário e o novo armazenamento secundário e certifique-se de que o estado do relacionamento esteja íntegro.
3. No SnapCenter, crie um backup dos recursos cujo armazenamento é migrado.

   Um novo backup é necessário para que o SnapCenter identifique a pegada de armazenamento mais recente e será usado para atualizar os metadados de backups antigos existentes.

   Você deve esperar até que esta operação seja concluída. Se você prosseguir para a próxima etapa antes da conclusão, o SnapCenter perderá completamente os metadados antigos do instantâneo secundário.

4. Após criar com sucesso o backup de todos os recursos em um host, execute a API de atualização de armazenamento secundário: `/<snapcenter_version>/techrefresh/secondarystorage` ou o cmdlet: *Invoke-SmTechRefreshSecondaryStorage*.

   Isso atualizará os detalhes do armazenamento secundário dos backups mais antigos no host fornecido.

   Se você quiser executar isso no nível do recurso, clique em **Atualizar** para cada recurso para atualizar os metadados do armazenamento secundário.

5. Depois de atualizar com sucesso os backups mais antigos, você pode quebrar o antigo relacionamento do armazenamento secundário com o primário.

Desinstalar o SnapCenter Server e os plug-ins

Desinstalar pacotes de plug-in SnapCenter

Pré-requisitos para remover um host

Você pode remover hosts e desinstalar plug-ins individuais ou pacotes de plug-ins usando a GUI do SnapCenter . Você também pode desinstalar plug-ins individuais ou pacotes de plug-ins em hosts remotos usando a interface de linha de comando (CLI) no seu host do SnapCenter Server ou usando a opção **Desinstalar um programa** do Windows localmente em qualquer host.

Antes de remover um host do SnapCenter Server, você deve concluir os pré-requisitos.

- Você deve efetuar login como administrador.
- Você deve garantir que os trabalhos de descoberta não estejam em execução no host.
- Você deve receber uma função com as permissões necessárias para remover todos os objetos associados ao host. Caso contrário, a operação de remoção falhará.
- Você deve confirmar a impressão digital se a chave SSH foi modificada após adicionar o host ao SnapCenter.
- Você deve confirmar a impressão digital se o host do SnapCenter for atualizado para uma versão posterior do SnapCenter , mas o host do plug-in ainda estiver executando uma versão anterior do plug-in.

Pré-requisitos para remover um host usando controle de acesso baseado em função

- Você deve ter efetuado login usando uma função RBAC que tenha permissões de leitura, exclusão de host, instalação, desinstalação de plug-in e exclusão de objetos.

  Os objetos podem ser clone, backup, grupo de recursos, sistema de armazenamento e assim por diante.

- Você deve ter adicionado o usuário RBAC à função RBAC.
- Você deve atribuir o usuário RBAC ao host, plug-in, credencial, grupos de recursos e sistema de armazenamento (para clones) que deseja excluir.
- Você deve ter efetuado login no SnapCenter como um usuário RBAC.

Pré-requisitos para remover um host com clones criados a partir da operação do ciclo de vida do clone

- Você deve ter criado trabalhos de clone usando o gerenciamento de ciclo de vida de clone para bancos de dados SQL.
- Você deve ter criado uma função RBAC com permissões de leitura e exclusão de clone, leitura e exclusão de recurso, leitura e exclusão de grupo de recursos, leitura e exclusão de armazenamento, leitura e exclusão de provisionamento, montagem, desmontagem, instalação e desinstalação de plug-in, leitura e exclusão de host.
- Você deve ter atribuído o usuário RBAC à função RBAC.
- Você deve ter atribuído o usuário RBAC ao host, ao SnapCenter Plug-in para Microsoft SQL Server, à credencial, ao grupo de recursos do ciclo de vida do clone e ao sistema de armazenamento.
- Você deve ter efetuado login no SnapCenter como um usuário RBAC.

Para obter informações sobre como desinstalar o SnapCenter Plug-in for VMware vSphere, consulte "Remover o SnapCenter Plug-in for VMware vSphere" .

Remover um host

Quando o SnapCenter Server remove um host, ele primeiro remove o backup, os clones, os trabalhos de clone, os grupos de recursos e os recursos listados para esse host na página Recursos do SnapCenter e, em seguida, desinstala os pacotes de plug-in no host.

Sobre esta tarefa

- Se você excluir um host, os backups, clones e grupos de recursos associados ao host também serão excluídos.
- Quando você remove os grupos de recursos, todos os agendamentos associados também são removidos.
- Se o host tiver um grupo de recursos compartilhado com outro host e você excluir o host, o grupo de recursos também será excluído.
- Você deve usar o cmdlet *Remove-SmHost* para remover os hosts de plug-in desativados ou inacessíveis.

  As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter"

- O tempo necessário para remover um host depende do número de backups e das configurações de retenção. Isso ocorre porque os Snapshots são excluídos de cada um dos controladores e os metadados são limpos.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página **Hosts**, clique em **Hosts gerenciados**.
3. Selecione o host que você deseja remover e clique em **Remover**.
4. Para clusters Oracle RAC, para remover o SnapCenter software de todos os hosts no cluster, selecione **Incluir todos os hosts do cluster**.

   Você também pode remover um nó de um cluster e, dessa forma, remover todos os nós, um por um.

5. Clique em **OK**.

> Quando você desinstala e reinstala plug-ins de host em um cluster, os recursos do cluster não são descobertos automaticamente. Selecione o nome do host do cluster e clique em **Atualizar recursos** para descobrir automaticamente os recursos do cluster.

Desinstalar plug-ins usando a interface gráfica do usuário do SnapCenter

Quando você decidir que não precisa mais de um plug-in individual ou de um pacote de plug-ins, poderá desinstalá-lo usando a interface do SnapCenter .

Antes de começar

- Você deve ter removido os grupos de recursos do pacote de plug-in que está desinstalando.

- Você deve ter desanexado as políticas associadas aos grupos de recursos do pacote de plug-in que está desinstalando.

Sobre esta tarefa

Você pode desinstalar um plug-in individual. Por exemplo, talvez seja necessário desinstalar o plug-in SnapCenter para Microsoft SQL Server porque um host está ficando sem recursos e você deseja mover esse plug-in para um host mais potente. Você também pode desinstalar um pacote de plug-in inteiro. Por exemplo, talvez seja necessário desinstalar o pacote de plug-ins do SnapCenter para Linux, que inclui o plug-in do SnapCenter para Oracle Database e o plug-in do SnapCenter para UNIX.

- Remover um host inclui desinstalar todos os plug-ins.

  Quando você remove um host do SnapCenter, o SnapCenter desinstala todos os pacotes de plug-in no host antes de removê-lo.

- A interface gráfica do usuário do SnapCenter remove plug-ins de um host por vez.

  Ao usar a interface gráfica do usuário do SnapCenter , você pode desinstalar plug-ins em apenas um host por vez. No entanto, você pode ter várias operações de desinstalação em execução ao mesmo tempo.

  Você também pode desinstalar um plug-in de vários hosts usando o cmdlet *Uninstall-SmHostPackage* e os parâmetros necessários. As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

> Desinstalar o pacote de plug-ins do SnapCenter para Windows de um host no qual o SnapCenter Server está instalado danificará a instalação do SnapCenter Server. Não desinstale o pacote de plug-ins do SnapCenter para Windows, a menos que tenha certeza de que não precisa mais do SnapCenter Server.

Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Na página Hosts gerenciados, selecione o host do qual você deseja desinstalar o plug-in ou pacote de plug-ins.
4. Ao lado do plug-in que você deseja remover, clique em **Remover** > **Enviar**.

Depois que você terminar

Você deve esperar 5 minutos antes de reinstalar o plug-in naquele host. Este período de tempo é suficiente para a GUI do SnapCenter atualizar o status do host gerenciado. A instalação falhará se você reinstalar o plug-in imediatamente.

Se você estiver desinstalando o pacote de plug-ins do SnapCenter para Linux, os arquivos de log específicos da desinstalação estarão disponíveis em: */custom_location/snapcenter/log*.

Desinstalar plug-ins do Windows usando o cmdlet do PowerShell

Você pode desinstalar plug-ins individuais ou desinstalar pacotes de plug-ins de um ou mais hosts usando o cmdlet *Uninstall-SmHostPackage* na interface de linha de comando do host do SnapCenter Server.

Você deve ter feito login no SnapCenter como um usuário de domínio com direitos de administrador local em cada host no qual deseja desinstalar os plug-ins.

Passos

1. Inicie o PowerShell.
2. No host do SnapCenter Server, digite: *Open-SMConnection -SMSbaseUrl https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME* command e, em seguida, insira suas credenciais.
3. Desinstale os plug-ins do Windows usando o cmdlet *Uninstall-SmHostPackage* e os parâmetros necessários.

   As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando *Get-Help command_name*. Alternativamente, você também pode consultar o "Guia de referência do cmdlet do software SnapCenter" .

Desinstalar plug-ins localmente em um host

Você pode desinstalar os plug-ins do SnapCenter localmente em um host se não conseguir acessar o host a partir do SnapCenter Server.

Sobre esta tarefa

A prática recomendada para desinstalar plug-ins individuais ou pacotes de plug-ins é usar a GUI do SnapCenter ou usar o cmdlet Uninstall-SmHostPackage na interface de linha de comando do host do SnapCenter Server. Esses procedimentos ajudam o SnapCenter Server a se manter atualizado com quaisquer alterações.

No entanto, você pode ter uma rara necessidade de desinstalar plug-ins localmente. Por exemplo, você pode ter executado uma tarefa de desinstalação do SnapCenter Server, mas a tarefa falhou, ou você desinstalou o SnapCenter Server e plug-ins órfãos permanecem em um host.

Desinstalar um pacote de plug-in localmente em um host não exclui dados associados ao host; por exemplo, trabalhos agendados e metadados de backup.

Não tente desinstalar o pacote de plug-ins do SnapCenter para Windows localmente pelo Painel de Controle. Você deve usar a interface gráfica do usuário do SnapCenter para garantir que o SnapCenter Plug-in para Microsoft Windows seja desinstalado corretamente.

Passos

1. No sistema host, navegue até o Painel de Controle e clique em **Desinstalar um programa**.
2. Na lista de programas, selecione o plug-in ou pacote de plug-ins do SnapCenter que você deseja desinstalar e clique em **Desinstalar**.

   O Windows desinstala todos os plug-ins no pacote selecionado.

Desinstalar pacote de plug-ins para Linux ou AIX usando CLI

Você pode desinstalar o SnapCenter Plug-ins Package para Linux ou o SnapCenter Plug-ins Package para AIX usando a interface de linha de comando.

Antes de começar

- Certifique-se de ter excluído os trabalhos agendados
- Certifique-se de que todos os trabalhos em execução sejam concluídos.

Etapa

Execute */custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall* para desinstalar.

Desinstalar o SnapCenter Server no host Windows

Se não desejar mais usar o SnapCenter Server para gerenciar tarefas de proteção de dados, você pode desinstalar o SnapCenter Server usando o Painel de Controle de Programas e Recursos no host do SnapCenter Server. Desinstalar o SnapCenter Server remove todos os seus componentes.

Antes de começar

- Certifique-se de ter pelo menos 2 GB de espaço livre na unidade onde o SnapCenter Server está instalado.
- Certifique-se de que o domínio no qual o SnapCenter Server está instalado não seja removido.

  Se você remover o domínio onde o SnapCenter Server foi instalado e tentar desinstalá-lo, a operação falhará.

- Você deve ter feito backup do banco de dados do repositório porque ele será limpo e desinstalado.

Passos

1. No host do SnapCenter Server, navegue até o Painel de Controle.
2. Certifique-se de que você está na visualização **Categoria**.
3. Em Programas, clique em **Desinstalar um programa**.

   A janela Programas e Recursos é aberta.

4. Selecione NetApp SnapCenter Server e clique em **Desinstalar**.

   A partir do SnapCenter 4.2, quando você desinstala o SnapCenter Server, todos os seus componentes, incluindo o banco de dados do repositório do MySQL Server, são desinstalados.

   - A remoção do nó NLB de um cluster NLB exige que você reinicie o host do SnapCenter Server. Se você não reiniciar o host, poderá ocorrer uma falha ao tentar reinstalar o SnapCenter Server.
   - Você deve desinstalar manualmente o .NET Framework, que não é removido durante a desinstalação.

Desinstalar o SnapCenter Server no host Linux

Se não desejar mais usar o SnapCenter Server para gerenciar tarefas de proteção de dados, você pode desinstalar o SnapCenter Server. Desinstalar o SnapCenter Server remove todos os seus componentes.

Passos

1. Execute uma das ações para desinstalar o SnapCenter Server.

Se você quiser executar…	Faça isso…
Desinstalação não interativa	`$ sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall -i silent -DCONFIRM=1` Exemplo: sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall
Desinstalação interativa	`$ sudo <USER_INSTALL_DIR>/NetApp/snapcenter/SnapManagerWeb/installation/uninstall` Digite qualquer valor diferente de 0 na entrada de confirmação para confirmar a desinstalação.

Automatize usando APIs REST

Automação do SnapCenter usando APIs REST

Você pode usar APIs REST para executar diversas operações de gerenciamento do SnapCenter . As APIs REST são expostas por meio da página da web do Swagger. Você pode acessar a página da web do Swagger disponível em *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/* para exibir a documentação da API REST, bem como para emitir manualmente uma chamada de API.

Os plug-ins que suportam APIs REST são:

- Plug-in para Microsoft SQL Server
- Plug-in para banco de dados SAP HANA
- Plug-in para banco de dados Oracle

Para obter informações sobre o SnapCenter Plug-in for VMware vSphere REST APIs, consulte "SnapCenter Plug-in for VMware vSphere"

Como acessar a API REST do SnapCenter nativamente

Você pode acessar a API REST do SnapCenter diretamente usando qualquer linguagem de programação que suporte um cliente REST. As opções de linguagem mais populares incluem Python, PowerShell e Java.

Fundação de serviços web REST

A Transferência de Estado Representacional (REST) é um estilo para a criação de aplicações web distribuídas. Quando aplicada ao design de uma API de serviços web, ela estabelece um conjunto de tecnologias e práticas recomendadas para expor recursos baseados em servidor e gerenciar seus estados. Ele usa protocolos e padrões convencionais para fornecer uma base flexível para gerenciar o SnapCenter.

Recursos e representação estatal

Os recursos são os componentes básicos de um sistema web. Ao criar uma aplicação de serviços web REST, as tarefas iniciais de design incluem:

Identificação de recursos baseados em sistema ou servidor

Todo sistema usa e mantém recursos. Um recurso pode ser um arquivo, uma transação comercial, um processo ou uma entidade administrativa. Uma das primeiras tarefas ao projetar uma aplicação baseada em serviços web REST é identificar os recursos.

Definição de estados de recursos e operações de estado associadas

Os recursos estão sempre em um de um número finito de estados. Os estados, bem como as operações associadas usadas para afetar as mudanças de estado, devem ser claramente definidos.

Pontos finais de URI

Cada recurso REST deve ser definido e disponibilizado usando um esquema de endereçamento bem definido. Os endpoints onde os recursos estão localizados e identificados usam um Identificador Uniforme de Recursos (URI).

O URI fornece uma estrutura geral para a criação de um nome exclusivo para cada recurso na rede. O Localizador Uniforme de Recursos (URL) é um tipo de URI usado com serviços web para identificar e acessar recursos. Os recursos são normalmente expostos em uma estrutura hierárquica semelhante a um diretório de arquivos.

Mensagens HTTP

O Protocolo de Transferência de Hipertexto (HTTP) é o protocolo usado pelo cliente e servidor de serviços web para trocar mensagens de solicitação e resposta sobre os recursos.

Como parte do design de um aplicativo de serviços web, os métodos HTTP são mapeados para os recursos e ações de gerenciamento de estado correspondentes. O HTTP não possui estado. Portanto, para associar um conjunto de solicitações e respostas relacionadas como parte de uma transação, informações adicionais devem ser incluídas nos cabeçalhos HTTP transportados com os fluxos de dados de solicitação e resposta.

Formatação JSON

Embora as informações possam ser estruturadas e transferidas entre um cliente e um servidor de serviços web de várias maneiras, a opção mais popular é a JavaScript Object Notation (JSON).

JSON é um padrão do setor para representar estruturas de dados simples em texto simples e é usado para transferir informações de estado que descrevem os recursos. A API REST do SnapCenter usa JSON para formatar os dados transportados no corpo de cada solicitação e resposta HTTP.

Características operacionais básicas

Embora o REST estabeleça um conjunto comum de tecnologias e práticas recomendadas, os detalhes de cada API podem variar de acordo com as escolhas de design.

Transação de API de solicitação e resposta

Cada chamada da API REST é realizada como uma solicitação HTTP ao sistema SnapCenter Server, que gera uma resposta associada ao cliente. Este par de solicitação e resposta é considerado uma transação de API.

Antes de usar a API, você deve estar familiarizado com as variáveis de entrada disponíveis para controlar uma solicitação e o conteúdo da saída da resposta.

Suporte para operações CRUD

Cada um dos recursos disponíveis por meio da API REST do SnapCenter é acessado com base no modelo CRUD:

- Criar
- Ler

- Atualizar
- Excluir

Para alguns recursos, apenas um subconjunto das operações é suportado.

Identificadores de objetos

Cada instância de recurso ou objeto recebe um identificador exclusivo quando é criado. Na maioria dos casos, o identificador é um UUID de 128 bits. Esses identificadores são globalmente exclusivos dentro de um SnapCenter Server específico.

Após emitir uma chamada de API que cria uma nova instância de objeto, uma URL com o ID associado é retornada ao chamador no cabeçalho de localização da resposta HTTP. Você pode extrair o identificador e usá-lo em chamadas subsequentes ao se referir à instância do recurso.

O conteúdo e a estrutura interna dos identificadores de objeto podem mudar a qualquer momento. Você deve usar os identificadores somente nas chamadas de API aplicáveis, conforme necessário, ao se referir aos objetos associados.

Instâncias e coleções de objetos

Dependendo do caminho do recurso e do método HTTP, uma chamada de API pode ser aplicada a uma instância de objeto específica ou a uma coleção de objetos.

Operações síncronas e assíncronas

O SnapCenter executa uma solicitação HTTP recebida de um cliente de forma síncrona ou assíncrona.

Processamento síncrono

O SnapCenter executa a solicitação imediatamente e responde com um código de status HTTP 200 ou 201 se for bem-sucedido.

Cada solicitação usando o método GET é sempre realizada de forma síncrona. Além disso, as solicitações que usam POST são projetadas para serem executadas de forma síncrona se a previsão for de que sejam concluídas em menos de dois segundos.

Processamento assíncrono

Se uma solicitação assíncrona for válida, o SnapCenter criará uma tarefa em segundo plano para processar a solicitação e um objeto de trabalho para ancorar a tarefa. O código de status HTTP 202 é retornado ao chamador junto com o objeto de trabalho. Você deve recuperar o estado do trabalho para determinar o sucesso ou o fracasso.

Solicitações que usam os métodos POST e DELETE são projetadas para serem executadas de forma assíncrona se a previsão é de que levem mais de dois segundos para serem concluídas.

Segurança

A segurança fornecida com a API REST é baseada principalmente nos recursos de segurança existentes disponíveis com o SnapCenter. A seguinte segurança é usada pela API:

Segurança da Camada de Transporte

Todo o tráfego enviado pela rede entre o SnapCenter Server e o cliente normalmente é criptografado usando TLS, com base nas configurações do SnapCenter .

Autenticação HTTP

No nível HTTP, a autenticação básica é usada para as transações da API. Um cabeçalho HTTP com o nome de usuário e a senha em uma string base64 é adicionado a cada solicitação.

Variáveis de entrada que controlam uma solicitação de API

Você pode controlar como uma chamada de API é processada por meio de parâmetros e variáveis definidos na solicitação HTTP.

Métodos HTTP

Os métodos HTTP suportados pela API REST do SnapCenter são mostrados na tabela a seguir.

Nem todos os métodos HTTP estão disponíveis em cada um dos pontos de extremidade REST.

Método HTTP	Descrição
PEGAR	Recupera propriedades de objeto em uma instância ou coleção de recursos.
PUBLICAR	Cria uma nova instância de recurso com base na entrada fornecida.
EXCLUIR	Exclui uma instância de recurso existente.
COLOCAR	Modifica uma instância de recurso existente.

Cabeçalhos de solicitação

Você deve incluir vários cabeçalhos na solicitação HTTP.

Tipo de conteúdo

Se o corpo da solicitação incluir JSON, este cabeçalho deverá ser definido como *application/json*.

Aceitar

Este cabeçalho deve ser definido como *application/json*.

Autorização

A autenticação básica deve ser definida com o nome de usuário e a senha codificados como uma string base64.

Corpo da solicitação

O conteúdo do corpo da solicitação varia dependendo da chamada específica. O corpo da solicitação HTTP

consiste em um dos seguintes:

- Objeto JSON com variáveis de entrada
- Vazio

Filtrando objetos

Ao emitir uma chamada de API que usa GET, você pode limitar ou filtrar os objetos retornados com base em qualquer atributo. Por exemplo, você pode especificar um valor exato para corresponder a:

```
<field>=<query value>
```

Além de uma correspondência exata, outros operadores estão disponíveis para retornar um conjunto de objetos em um intervalo de valores. A API REST do SnapCenter suporta os operadores de filtragem mostrados na tabela abaixo.

Operador	Descrição
=	Igual a
<	Menor que
>	Maior que
⇐	Menor ou igual a
>=	Maior ou igual a
ATUALIZAR	Ou
!	Não é igual a
*	Curinga ganancioso

Você também pode retornar uma coleção de objetos com base em se um campo específico está definido ou não usando a palavra-chave **null** ou sua negação **!null** como parte da consulta.

Todos os campos que não são definidos geralmente são excluídos das consultas correspondentes.

Solicitando campos de objetos específicos

Por padrão, emitir uma chamada de API usando GET retorna apenas os atributos que identificam exclusivamente o(s) objeto(s). Esse conjunto mínimo de campos atua como uma chave para cada objeto e varia de acordo com o tipo de objeto. Você pode selecionar propriedades adicionais do objeto usando o `fields` parâmetro de consulta das seguintes maneiras:

Campos comuns ou padrão

Especifique **fields=*** para recuperar os campos de objeto mais comumente usados. Esses campos geralmente são mantidos na memória do servidor local ou exigem pouco processamento para acesso. Essas são as mesmas propriedades retornadas para um objeto após usar GET com uma chave de caminho de URL (UUID).

Todos os campos

Especifique **fields=*** para recuperar todos os campos do objeto, incluindo aqueles que exigem processamento adicional do servidor para acesso.

Seleção de campo personalizado

Use **fields=<nome_do_campo>** para especificar o campo exato que você deseja. Ao solicitar vários campos, os valores devem ser separados por vírgulas, sem espaços.

> Como prática recomendada, você deve sempre identificar os campos específicos que deseja. Você deve recuperar somente o conjunto de campos comuns ou todos os campos quando necessário. Quais campos são classificados como comuns e retornados usando *fields=** são determinados pela NetApp com base na análise de desempenho interna. A classificação de um campo pode mudar em versões futuras.

Classificando objetos no conjunto de saída

Os registros em uma coleção de recursos são retornados na ordem padrão definida pelo objeto. Você pode alterar a ordem usando o `order_by` parâmetro de consulta com o nome do campo e a direção de classificação da seguinte forma:

```
order_by=<field name> asc|desc
```

Por exemplo, você pode classificar o campo tipo em ordem decrescente seguido pelo id em ordem crescente:

```
order_by=type desc, id asc
```

- Se você especificar um campo de classificação, mas não fornecer uma direção, os valores serão classificados em ordem crescente.
- Ao incluir vários parâmetros, você deve separar os campos com uma vírgula.

Paginação ao recuperar objetos em uma coleção

Ao emitir uma chamada de API usando GET para acessar uma coleção de objetos do mesmo tipo, o SnapCenter tenta retornar o máximo de objetos possível com base em duas restrições. Você pode controlar cada uma dessas restrições usando parâmetros de consulta adicionais na solicitação. A primeira restrição atingida para uma solicitação GET específica encerra a solicitação e, portanto, limita o número de registros retornados.

> Se uma solicitação terminar antes de iterar sobre todos os objetos, a resposta conterá o link necessário para recuperar o próximo lote de registros.

Limitando o número de objetos

Por padrão, o SnapCenter retorna no máximo 10.000 objetos para uma solicitação GET. Você pode alterar esse limite usando o parâmetro de consulta *max_records*. Por exemplo:

```
max_records=20
```

O número de objetos realmente retornados pode ser menor que o máximo em vigor, com base na restrição de tempo relacionada, bem como no número total de objetos no sistema.

Limitar o tempo usado para recuperar os objetos

Por padrão, o SnapCenter retorna o máximo de objetos possível dentro do tempo permitido para a solicitação GET. O tempo limite padrão é 15 segundos. Você pode alterar esse limite usando o parâmetro de consulta *return_timeout*. Por exemplo:

```
return_timeout=5
```

O número de objetos realmente retornados pode ser menor que o máximo em vigor, com base na restrição relacionada ao número de objetos, bem como no número total de objetos no sistema.

Estreitando o conjunto de resultados

Se necessário, você pode combinar esses dois parâmetros com parâmetros de consulta adicionais para restringir o conjunto de resultados. Por exemplo, o seguinte retorna até 10 eventos EMS gerados após o tempo especificado:

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

Você pode emitir várias solicitações para percorrer os objetos. Cada chamada de API subsequente deve usar um novo valor de tempo com base no evento mais recente no último conjunto de resultados.

Propriedades de tamanho

Os valores de entrada usados com algumas chamadas de API, bem como certos parâmetros de consulta, são numéricos. Em vez de fornecer um número inteiro em bytes, você pode usar um sufixo, conforme mostrado na tabela a seguir.

Sufixo	Descrição
KB	KB Kilobytes (1024 bytes) ou kibibytes
MB	MB Megabytes (KB x 1024 bytes) ou mebibytes
GB	GB Gigabytes (MB x 1024 bytes) ou gibibytes
tuberculose	TB Terabytes (GB x 1024 bytes) ou tebibytes
PB	PB Petabytes (TB x 1024 bytes) ou pebibytes

Interpretação de uma resposta de API

Cada solicitação de API gera uma resposta ao cliente. Você deve examinar a resposta para determinar se ela foi bem-sucedida e recuperar dados adicionais conforme necessário.

Código de status HTTP

Os códigos de status HTTP usados pela API REST do SnapCenter são descritos abaixo.

Código	Descrição
200	OK Indica sucesso para chamadas que não criam um novo objeto.

Código	Descrição
201	Criado Um objeto foi criado com sucesso. O cabeçalho de localização na resposta inclui o identificador exclusivo do objeto.
202	Aceito Um trabalho em segundo plano foi iniciado para executar a solicitação, mas ainda não foi concluído.
400	Solicitação incorreta A entrada da solicitação não é reconhecida ou é inadequada.
401	A autenticação do usuário não autorizado falhou.
403	Acesso proibido negado devido a um erro de autorização (RBAC).
404	Não encontrado O recurso mencionado na solicitação não existe.
405	Método não permitido O método HTTP na solicitação não é suportado para o recurso.
409	Conflito Uma tentativa de criar um objeto falhou porque um objeto diferente deve ser criado primeiro ou o objeto solicitado já existe.
500	Erro interno Ocorreu um erro interno geral no servidor.

Cabeçalhos de resposta

Vários cabeçalhos são incluídos na resposta HTTP gerada pelo SnapCenter.

Localização

Quando um objeto é criado, o cabeçalho de localização inclui o URL completo para o novo objeto, incluindo o identificador exclusivo atribuído ao objeto.

Tipo de conteúdo

Isso normalmente será `application/json` .

Corpo de resposta

O conteúdo do corpo de resposta resultante de uma solicitação de API difere com base no objeto, no tipo de processamento e no sucesso ou falha da solicitação. A resposta é sempre renderizada em JSON.

Objeto único

Um único objeto pode ser retornado com um conjunto de campos com base na solicitação. Por exemplo, você pode usar GET para recuperar propriedades selecionadas de um cluster usando o identificador exclusivo.

Vários objetos

Vários objetos de uma coleção de recursos podem ser retornados. Em todos os casos, há um formato consistente usado, com `num_records` indicando o número de registros e registros contendo uma matriz de instâncias do objeto. Por exemplo, você pode recuperar os nós definidos em um cluster específico.

Objeto de trabalho

Se uma chamada de API for processada de forma assíncrona, um objeto Job será retornado, ancorando a tarefa em segundo plano. Por exemplo, a solicitação PATCH usada para atualizar a configuração do cluster é processada de forma assíncrona e retorna um objeto Job.

Objeto de erro

Se ocorrer um erro, um objeto Error será sempre retornado. Por exemplo, você receberá um erro ao tentar alterar um campo não definido para um cluster.

Vazio

Em certos casos, nenhum dado é retornado e o corpo da resposta inclui um objeto JSON vazio.

Erros

Se ocorrer um erro, um objeto de erro será retornado no corpo da resposta.

Formatar

Um objeto de erro tem o seguinte formato:

```
"error": {
"message": "<string>",
"code": <integer>[,
"target": "<string>"]
}
```

Você pode usar o valor do código para determinar o tipo ou categoria geral de erro, e a mensagem para determinar o erro específico. Quando disponível, o campo de destino inclui a entrada específica do usuário associada ao erro.

Códigos de erro comuns

Os códigos de erro comuns são descritos na tabela a seguir. Chamadas de API específicas podem incluir códigos de erro adicionais.

Código	Descrição
409	Já existe um objeto com o mesmo identificador.
400	O valor de um campo tem um valor inválido ou está ausente, ou um campo extra foi fornecido.
400	A operação não é suportada.

Código	Descrição
405	Um objeto com o identificador especificado não pode ser encontrado.
403	A permissão para executar a solicitação foi negada.
409	O recurso está em uso.

APIs REST suportadas pelo SnapCenter Server e plug-ins

Os recursos disponíveis por meio da API REST do SnapCenter são organizados em categorias, conforme exibido na página de documentação da API do SnapCenter . Uma breve descrição de cada um dos recursos com os caminhos de recursos básicos é apresentada abaixo, juntamente com considerações adicionais de uso, quando apropriado.

Aut.

Você pode usar esta API para fazer login no SnapCenter Server. Esta API retorna um token de autorização do usuário que é usado para autenticar solicitações subsequentes.

Domínios

Você pode usar APIs para executar diferentes operações.

- recuperar todos os domínios no SnapCenter
- recuperar detalhes de um domínio específico
- registrar ou cancelar o registro de um domínio
- modificar um domínio

Empregos

Você pode usar APIs para executar diferentes operações.

- recuperar todos os trabalhos no SnapCenter
- recuperar status de um trabalho
- cancelar ou parar um trabalho

Configurações

Você pode usar APIs para executar diferentes operações.

- registrar, modificar ou remover uma credencial
- exibe as informações de credenciais registradas no SnapCenter Server
- configurar configurações de notificação
- recupera informações sobre o servidor SMTP atualmente configurado para enviar notificações por e-mail e exibe o nome do servidor SMTP, o nome dos destinatários e o nome do remetente

- exibe a configuração de autenticação multifator (MFA) do login do SnapCenter Server
- habilitar ou desabilitar e configurar o MFA para o login do SnapCenter Server
- crie o arquivo de configuração necessário para configurar o MFA

Anfitriões

Você pode usar APIs para executar diferentes operações.

- consultar todos os hosts SnapCenter
- remover um ou mais hosts do SnapCenter
- recuperar um host pelo nome
- recuperar todos os recursos em um host
- recuperar um recurso usando o ID do recurso
- recuperar os detalhes de configuração do plug-in
- configurar o host do plug-in
- recuperar todos os recursos do plug-in para o host do Microsoft SQL Server
- recuperar todos os recursos do plug-in para o host do banco de dados Oracle
- recuperar todos os recursos do plug-in para host de aplicativo personalizado
- recuperar todos os recursos do plug-in para o host SAP HANA
- recuperar os plug-ins instalados
- instalar plug-ins em um host existente
- atualizar pacote de host
- remover plug-ins de um host existente
- adicionar plug-in em um host
- adicionar ou modificar host
- obter a assinatura do host Linux
- registrar a assinatura do host Linux
- coloque o host em modo de manutenção ou produção
- iniciar ou reiniciar os serviços de plug-in no host
- renomear um host

Recursos

Você pode usar APIs para executar diferentes operações.

- recuperar todos os recursos
- recuperar um recurso usando o ID do recurso
- recuperar todos os recursos do plug-in para o host do Microsoft SQL Server
- recuperar todos os recursos do plug-in para o host do banco de dados Oracle
- recuperar todos os recursos do plug-in para host de aplicativo personalizado
- recuperar todos os recursos do plug-in para o host SAP HANA

- recuperar um recurso do Microsoft SQL Server usando uma chave
- recuperar um recurso personalizado usando uma chave
- modificar um recurso do plug-in para host de aplicativo personalizado
- remover um recurso do plug-in para host de aplicativo personalizado usando uma chave
- recuperar um recurso SAP HANA usando uma chave
- modificar um recurso do plug-in para host SAP HANA
- remover um recurso do plug-in para host SAP HANA usando uma chave
- recuperar um recurso Oracle usando uma chave
- criar um recurso de volume de aplicativo Oracle
- modificar um recurso de volume do aplicativo Oracle
- remover um recurso de volume do aplicativo Oracle usando uma chave
- recuperar os detalhes secundários do recurso Oracle
- faça backup do recurso do Microsoft SQL Server usando o plug-in para Microsoft SQL Server
- faça backup do recurso Oracle usando o plug-in para banco de dados Oracle
- faça backup do recurso personalizado usando o plug-in para aplicativo personalizado
- configurar o banco de dados SAP HANA
- configurar o banco de dados Oracle
- restaurar um backup de banco de dados SQL
- restaurar um backup de banco de dados Oracle
- restaurar um backup de aplicativo personalizado
- criar um recurso SAP HANA
- proteger um recurso personalizado usando plug-in para aplicativo personalizado
- proteger um recurso do Microsoft SQL Server usando o plug-in para Microsoft SQL Server
- modificar um recurso protegido do Microsoft SQL Server
- remover proteção para recurso do Microsoft SQL Server
- proteger um recurso Oracle usando plug-in para banco de dados Oracle
- modificar um recurso Oracle protegido
- remover proteção do recurso Oracle
- clonar um recurso do backup usando plug-in para aplicativo personalizado
- clonar um volume de aplicativo Oracle do backup usando o plug-in para banco de dados Oracle
- clonar um recurso do Microsoft SQL Server do backup usando o plug-in para Microsoft SQL Server
- criar um ciclo de vida clone de um recurso do Microsoft SQL Server
- modificar o ciclo de vida do clone de um recurso do Microsoft SQL Server
- excluir ciclo de vida do clone de um recurso do Microsoft SQL Server
- mover um banco de dados Microsoft SQL Server existente de um disco local para um LUN NetApp
- crie um arquivo de especificação de clone para um banco de dados Oracle
- iniciar um trabalho de atualização de clone sob demanda de um recurso Oracle

- crie um recurso Oracle a partir do backup usando o arquivo de especificação do clone
- restaura o banco de dados para a réplica secundária e une o banco de dados de volta ao grupo de disponibilidade
- criar um recurso de volume de aplicativo Oracle

Backups

Você pode usar APIs para executar diferentes operações.

- recuperar detalhes de backup por nome, tipo, plug-in, recurso ou data
- recuperar todos os backups
- recuperar detalhes de backup
- renomear ou excluir backups
- montar um backup Oracle
- desmontar um backup Oracle
- catalogar um backup Oracle
- descatalogar um backup Oracle
- obtenha todos os backups necessários para serem montados para executar a recuperação pontual

Clones

Você pode usar APIs para executar diferentes operações.

- criar, exibir, modificar e excluir arquivo de especificação de clone do banco de dados Oracle
- exibir hierarquia de clones do banco de dados Oracle
- recuperar detalhes do clone
- recuperar todos os clones
- excluir clones
- recuperar detalhes do clone por ID
- iniciar um trabalho de atualização de clone sob demanda de um recurso Oracle
- clonar um recurso Oracle do backup usando o arquivo de especificação de clone

Divisão do clone

Você pode usar APIs para executar diferentes operações.

- estimar a operação de divisão do clone do recurso clonado
- recuperar o status de uma operação de divisão de clone
- iniciar ou parar uma operação de divisão de clone

Grupos de Recursos

Você pode usar APIs para executar diferentes operações.

- recuperar detalhes de todos os grupos de recursos

- recuperar o grupo de recursos pelo nome
- criar um grupo de recursos para plug-in para aplicativo personalizado
- criar um grupo de recursos para plug-in para Microsoft SQL Server
- criar um grupo de recursos para plug-in para banco de dados Oracle
- modificar um grupo de recursos para plug-in para aplicativo personalizado
- modificar um grupo de recursos para plug-in para Microsoft SQL Server
- modificar um grupo de recursos para plug-in para banco de dados Oracle
- criar, modificar ou excluir o ciclo de vida do clone de um grupo de recursos para plug-in do Microsoft SQL Server
- fazer backup de um grupo de recursos
- coloque o grupo de recursos no modo de manutenção ou produção
- remover um grupo de recursos

Políticas

Você pode usar APIs para executar diferentes operações.

- recuperar detalhes da política
- recuperar detalhes da política por nome
- excluir uma política
- criar uma cópia de uma política existente
- criar ou modificar política para plug-in para aplicativo personalizado
- criar ou modificar política para plug-in para Microsoft SQL Server
- criar ou modificar política para plug-in para banco de dados Oracle
- criar ou modificar política para plug-in para banco de dados SAP HANA

Armazenar

Você pode usar APIs para executar diferentes operações.

- recuperar todas as ações
- recuperar um compartilhamento pelo nome
- criar ou excluir um compartilhamento
- recuperar detalhes de armazenamento
- recuperar detalhes de armazenamento por nome
- criar, modificar ou excluir um armazenamento
- descobrir recursos em um cluster de armazenamento
- recuperar recursos em um cluster de armazenamento

Compartilhar

Você pode usar APIs para executar diferentes operações.

- recuperar os detalhes de um compartilhamento
- recuperar detalhes de todas as ações
- criar ou excluir um compartilhamento no armazenamento
- recuperar um compartilhamento pelo nome

Plugins

Você pode usar APIs para executar diferentes operações.

- listar todos os plug-ins para um host
- recuperar um recurso do Microsoft SQL Server usando uma chave
- modificar um recurso personalizado usando uma chave
- remover um recurso personalizado usando uma chave
- recuperar um recurso SAP HANA usando uma chave
- modificar um recurso SAP HANA usando uma chave
- remover um recurso SAP HANA usando uma chave
- recuperar um recurso Oracle usando uma chave
- modificar um recurso de volume do aplicativo Oracle usando uma chave
- remover um recurso de volume do aplicativo Oracle usando uma chave
- faça backup do recurso do Microsoft SQL Server usando o plug-in para Microsoft SQL Server e uma chave
- faça backup do recurso Oracle usando o plug-in para banco de dados Oracle e uma chave
- faça backup do recurso do aplicativo personalizado usando o plug-in para aplicativo personalizado e uma chave
- configurar o banco de dados SAP HANA usando uma chave
- configurar o banco de dados Oracle usando uma chave
- restaurar um backup de aplicativo personalizado usando uma chave
- criar um recurso SAP HANA
- criar um recurso de volume de aplicativo Oracle
- proteger um recurso personalizado usando plug-in para aplicativo personalizado
- proteger um recurso do Microsoft SQL Server usando o plug-in para Microsoft SQL Server
- modificar um recurso protegido do Microsoft SQL Server
- remover proteção para recurso do Microsoft SQL Server
- proteger um recurso Oracle usando plug-in para banco de dados Oracle
- modificar um recurso Oracle protegido
- remover proteção do recurso Oracle
- clonar um recurso do backup usando plug-in para aplicativo personalizado
- clonar um volume de aplicativo Oracle do backup usando o plug-in para banco de dados Oracle
- clonar um recurso do Microsoft SQL Server do backup usando o plug-in para Microsoft SQL Server
- criar um ciclo de vida clone de um recurso do Microsoft SQL Server

- modificar o ciclo de vida do clone de um recurso do Microsoft SQL Server
- excluir ciclo de vida do clone de um recurso do Microsoft SQL Server
- crie um arquivo de especificação de clone para um banco de dados Oracle
- iniciar um ciclo de vida de clone sob demanda de um recurso Oracle
- clonar um recurso Oracle do backup usando o arquivo de especificação de clone

Relatórios

Você pode usar APIs para executar diferentes operações.

- recuperar relatórios de operações de backup, restauração e clonagem para os respectivos plug-ins
- adicionar, executar, excluir ou modificar programações
- recuperar dados para os relatórios agendados

Alertas

Você pode usar APIs para executar diferentes operações.

- recuperar todos os alertas
- recuperar alertas por IDs
- excluir vários alertas ou excluir um alerta por ID

RBAC

Você pode usar APIs para executar diferentes operações.

- recuperar detalhes de usuários, grupos e funções
- adicionar ou excluir usuários
- atribuir usuário à função
- desatribuir usuário da função
- criar, modificar ou excluir funções
- atribuir grupo a uma função
- remover atribuição de grupo de uma função
- adicionar ou excluir grupos
- criar uma cópia de uma função existente
- atribuir ou desatribuir recursos ao usuário ou grupo

Configuração

Você pode usar APIs para executar diferentes operações.

- ver as configurações
- modificar as configurações

Configurações do Certificado

Você pode usar APIs para executar diferentes operações.

- visualizar o status do certificado do SnapCenter Server ou do host do plug-in
- modificar as configurações do certificado para o SnapCenter Server ou host do plug-in

Repositório

Você pode usar APIs para executar diferentes operações.

- recuperar os backups do repositório
- visualizar as informações de configuração sobre o repositório
- proteger e restaurar o repositório SnapCenter
- desproteger o repositório SnapCenter
- reconstruir e fazer failover do repositório

Versão

Você pode usar esta API para visualizar a versão do SnapCenter .

Como acessar APIs REST usando a página da web da API do Swagger

As APIs REST são expostas por meio da página da web do Swagger. Você pode acessar a página da web do Swagger para exibir as APIs REST do SnapCenter Server, bem como emitir manualmente uma chamada de API. Você pode usar APIs REST para ajudar a gerenciar seu SnapCenter Server ou para executar operações de proteção de dados.

Você deve saber o endereço IP de gerenciamento ou o nome de domínio do SnapCenter Server no qual deseja executar as APIs REST.

Você não precisa de permissões especiais para executar o cliente da API REST. Qualquer usuário pode acessar a página web do Swagger. As respectivas permissões nos objetos acessados via API REST são baseadas no usuário que gera o token para efetuar login na API REST.

Passos

1. Em um navegador, insira o URL para acessar a página da web do Swagger no formato *https://<endereço_IP_ou_nome_do_SnapCenter>:<porta_do_SnapCenter>/swagger/*.

   Certifique-se de que a URL da API REST não tenha os seguintes caracteres: +, ., % e &.

2. No campo **Swagger Explore**, se a documentação da API do Swagger não for exibida automaticamente, digite: *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/Content/swagger/SnapCenter.yaml*
3. Clique em **Explorar**.

   Uma lista de tipos ou categorias de recursos de API é exibida.

4. Clique em um tipo de recurso de API para exibir as APIs nesse tipo de recurso.

Se você encontrar um comportamento inesperado ao executar as APIs REST do SnapCenter , poderá usar os arquivos de log para identificar a causa e resolver o problema. Você pode baixar os arquivos de log da interface do usuário do SnapCenter clicando em **Monitor** > **Logs** > **Download**.

Comece a usar a API REST

Você pode começar rapidamente usando a API REST do SnapCenter . Acessar a API fornece alguma perspectiva antes de você começar a usá-la com processos de fluxo de trabalho mais complexos em uma configuração ativa.

Olá Mundo

Você pode executar um comando simples no seu sistema para começar a usar a API REST do SnapCenter e confirmar sua disponibilidade.

Antes de começar

- Certifique-se de que o utilitário Curl esteja disponível no seu sistema.
- Endereço IP ou nome do host do SnapCenter Server
- Nome de usuário e senha para uma conta com autoridade para acessar a API REST do SnapCenter .

> Se suas credenciais incluírem caracteres especiais, você precisará formatá-las de uma forma que seja aceitável para o Curl com base no shell que você está usando. Por exemplo, você pode inserir uma barra invertida antes de cada caractere especial ou quebrar todo o caractere `username:password` string entre aspas simples.

Etapa

Na interface de linha de comando, execute o seguinte para recuperar as informações do plug-in:

```
curl -X GET -u username:password -k
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

Exemplo:

```
curl -X GET -u admin:password -k
"'https://10.225.87.97/api/hosts?fields=IncludePluginInfo"
```

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos autorais

"https://www.netapp.com/company/legal/copyright/"

Marcas Registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas de seus respectivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de Privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais e licenças de terceiros usados no software NetApp .

"Aviso para SnapCenter 6.1"

Informações sobre direitos autorais

Informações sobre marcas comerciais