Documentação do software SnapCenter

SnapCenter Software 6.0

NetApp
November 06, 2025

This PDF was generated from https://docs.netapp.com/pt-br/snapcenter-60/index.html on November 06, 2025. Always check docs.netapp.com for the latest.

Índice

Documentação do software SnapCenter . . . 1
Notas de lançamento . . . 2
  Notas de lançamento . . . 2
  Caminhos de atualização compatíveis para o SnapCenter . . . 2
Conceitos . . . 3
  Visão geral do SnapCenter . . . 3
    Arquitetura da SnapCenter . . . 6
    Componentes do SnapCenter . . . 6
    Servidor SnapCenter . . . 7
    Plug-ins do SnapCenter . . . 8
    Repositório SnapCenter . . . 11
  Recursos de segurança . . . 11
    Visão geral do certificado CA . . . 12
    Comunicação SSL bidirecional . . . 13
    Visão geral da autenticação baseada em certificados . . . 13
    Autenticação multifator (MFA) . . . 13
  Controles de acesso baseados em função do SnapCenter (RBAC) . . . 13
    Tipos de RBAC . . . 13
    Permissões e funções do RBAC . . . 15
    Funções e permissões do SnapCenter predefinidas . . . 16
  Recuperação de desastres do SnapCenter . . . 20
  Recursos, grupos de recursos e políticas . . . 21
  Prescripts e postscripts . . . 22
    Tipos de script suportados . . . 22
    Caminho do script . . . 23
    Onde especificar scripts . . . 23
    Tempos limite de script . . . 23
    Saída de script . . . 23
  Automação da SnapCenter usando APIS REST . . . 23
Instalação do servidor SnapCenter . . . 25
  Fluxo de trabalho de instalação . . . 25
  Prepare-se para instalar o servidor SnapCenter . . . 25
    Requisitos de domínio e grupo de trabalho . . . 25
    Requisitos de espaço e dimensionamento . . . 26
    Requisitos de host SAN . . . 27
    Sistemas e aplicações de storage compatíveis . . . 28
    Navegadores suportados . . . 28
    Requisitos de conexão e porta . . . 29
    Licenças SnapCenter . . . 32
    Registe-se para aceder ao software SnapCenter . . . 35
    Métodos de autenticação para suas credenciais . . . 35
    Conexões e credenciais de storage . . . 36
    Autenticação multifator (MFA) . . . 37

Instale o servidor SnapCenter no host Windows . . . 47
Registre o produto para habilitar o suporte . . . 48
Instale o servidor SnapCenter no host Linux . . . 49
Registre o produto para habilitar o suporte . . . 53
Faça login no SnapCenter usando a autorização RBAC . . . 53
Faça login no SnapCenter usando autenticação multifator (MFA) . . . 55
Modifique o tempo limite padrão da sessão da GUI do SnapCenter . . . 56
Proteja o servidor web SnapCenter desativando o SSL 3,0 . . . 56
Configurar o certificado CA para o host Windows . . . 56
Gerar arquivo CSR do certificado CA . . . 56
Importar certificados CA . . . 57
Obtenha a impressão digital do certificado CA . . . 58
Configure o certificado CA com os serviços de plug-in do host do Windows . . . 58
Configure o certificado CA com o site SnapCenter . . . 59
Ativar certificados de CA para SnapCenter . . . 60
Configure o certificado CA para o host Linux . . . 60
Configure o certificado nginx . . . 60
Configurar o certificado de log de auditoria . . . 61
Configurar o certificado de serviços SnapCenter . . . 61
Configure e ative a comunicação SSL bidirecional no host Windows . . . 61
Configurar comunicação SSL bidirecional no host Windows . . . 61
Ative a comunicação SSL bidirecional no host Windows . . . 64
Configure e habilite a comunicação SSL bidirecional no host Linux . . . 65
Configurar comunicação SSL bidirecional no host Linux . . . 65
Ative a comunicação SSL no host Linux . . . 67
Configurar autenticação baseada em certificado . . . 67
Exportar certificados de autoridade de certificação (CA) do servidor SnapCenter . . . 67
Importar certificado de autoridade de certificação (CA) para os hosts de plug-in do Windows . . . 68
Importe o certificado CA para os plug-ins do host UNIX e configure certificados raiz ou intermediários para o armazenamento de confiança SPL . . . 69
Ativar autenticação baseada em certificado . . . 70
Exportar certificados SnapCenter . . . 71
Configure o ative Directory, LDAP e LDAPS . . . 72
Registre domínios não confiáveis do ative Directory . . . 72
Configure o certificado de cliente CA para LDAPS . . . 73
Configurar alta disponibilidade . . . 74
Configurar servidores SnapCenter para alta disponibilidade . . . 74
Alta disponibilidade para o repositório SnapCenter MySQL . . . 78
Configurar controles de acesso baseados em função (RBAC) . . . 79
Adicione um usuário ou grupo e atribua funções e ativos . . . 79
Crie uma função . . . 82
Adicione uma função ONTAP RBAC usando comandos de login de segurança . . . 82
Criar funções do SVM com Privileges mínimo . . . 84
Criar funções de cluster do ONTAP com Privileges mínimo . . . 89
Configure pools de aplicativos do IIS para habilitar permissões de leitura do ative Directory . . . 95

Configurar as definições do registo de auditoria . . . 96
Adicione sistemas de storage . . . 97
Adicione licenças padrão baseadas em controladora SnapCenter . . . 101
Etapa 1: Verifique se a licença do SnapManager Suite está instalada . . . 101
Passo 2: Identifique as licenças instaladas no controlador . . . 102
Passo 3: Recupere o número de série do controlador . . . 103
Passo 4: Recupere o número de série da licença baseada no controlador . . . 104
Passo 5: Adicione licença baseada no controlador . . . 105
Passo 6: Remova a licença de teste . . . 106
Provisione seu sistema de storage . . . 106
Provisione storage em hosts do Windows . . . 106
Provisione storage em ambientes VMware . . . 122
Configure conexões MySQL seguras com o servidor SnapCenter . . . 124
Configurar conexões MySQL seguras para configurações autônomas do servidor SnapCenter . . . 124
Configurar conexões MySQL seguras para configurações HA . . . 126
Recursos ativados em seu host Windows durante a instalação . . . 130
Recursos ativados no host Linux durante a instalação . . . 133
Proteja bancos de dados Microsoft SQL Server . . . 134
Plug-in do SnapCenter para Microsoft SQL Server . . . 134
Visão geral do plug-in do SnapCenter para Microsoft SQL Server . . . 134
O que você pode fazer com o plug-in SnapCenter para Microsoft SQL Server . . . 134
Plug-in do SnapCenter para recursos do Microsoft SQL Server . . . 135
Suporte para mapeamento LUN assimétrico em clusters Windows . . . 136
Tipos de storage compatíveis com o plug-in SnapCenter para Microsoft SQL Server . . . 137
Recomendações de layout de storage para o plug-in SnapCenter para Microsoft SQL Server . . . 140
ONTAP Privileges mínimo necessário para plug-in SQL . . . 142
Preparar sistemas de storage para replicação SnapMirror e SnapVault para plug-in para SQL Server . . . 144
Estratégia de backup para recursos do SQL Server . . . 145
Estratégia de restauração para SQL Server . . . 149
Defina uma estratégia de clonagem para o SQL Server . . . 153
Prepare-se para instalar o plug-in do SnapCenter para Microsoft SQL Server . . . 154
Fluxo de trabalho de instalação para o plug-in SnapCenter para Microsoft SQL Server . . . 154
Pré-requisitos para adicionar hosts e instalar o plug-in do SnapCenter para Microsoft SQL Server . . . 154
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows . . . 155
Configure credenciais para o pacote de plug-ins do SnapCenter para Windows . . . 156
Configurar credenciais para um recurso do SQL Server individual . . . 157
Configure o gMSA no Windows Server 2016 ou posterior . . . 160
Instale o plug-in do SnapCenter para Microsoft SQL Server . . . 161
Configurar certificado CA . . . 167
Configurar a recuperação de desastres . . . 170
Instale o plug-in do SnapCenter para VMware vSphere . . . 172
Implantar certificado CA . . . 172
Configure o arquivo CRL . . . 173
Preparar-se para a proteção de dados . . . 173
Pré-requisitos para usar o plug-in do SnapCenter para Microsoft SQL Server . . . 173

Como recursos, grupos de recursos e políticas são usados para proteger o SQL Server . . . 174
Faça backup do banco de dados do SQL Server, instância ou grupo de disponibilidade . . . 175
Fluxo de trabalho de backup . . . 175
Determine se os recursos estão disponíveis para backup . . . 176
Migrar recursos para o sistema de storage NetApp . . . 177
Criar políticas de backup para bancos de dados do SQL Server . . . 179
Crie grupos de recursos e anexe políticas para o SQL Server . . . 187
Requisitos para fazer backup de recursos SQL . . . 190
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell . . . 190
Faça backup de recursos SQL . . . 191
Fazer backup de grupos de recursos do SQL Server . . . 196
Monitore operações de backup de recursos SQL na página de tarefas do SnapCenter . . . 197
Cancele o plug-in do SnapCenter para operações de backup do Microsoft SQL Server . . . 198
Veja os backups e clones do SQL Server na página topologia . . . 199
Limpe a contagem de backup secundária usando cmdlets do PowerShell . . . 201
Restaurar recursos do SQL Server . . . 201
Restaure o fluxo de trabalho . . . 201
Requisitos para restaurar um banco de dados . . . 202
Restaure backups de banco de dados do SQL Server . . . 203
Restaure um banco de dados SQL Server a partir do armazenamento secundário . . . 210
Restaure recursos usando cmdlets do PowerShell . . . 211
Reseed Availability Group Databases . . . 213
Monitorar operações de restauração de recursos SQL . . . 214
Cancelar operações de restauração de recursos SQL . . . 215
Clonar recursos de banco de dados do SQL Server . . . 215
Fluxo de trabalho clone . . . 216
Clone de um backup de banco de dados do SQL Server . . . 216
Execute o ciclo de vida do clone . . . 224
Monitorar operações de clone de banco de dados SQL . . . 227
Cancelar operações de clone de recursos SQL . . . 227
Divida um clone . . . 228
Proteger bancos de dados SAP HANA . . . 230
Plug-in do SnapCenter para bancos de dados SAP HANA . . . 230
Visão geral do plug-in do SnapCenter para banco de dados SAP HANA . . . 230
O que você pode fazer usando o plug-in do SnapCenter para banco de dados SAP HANA . . . 230
Plug-in do SnapCenter para recursos de banco de dados SAP HANA . . . 230
Tipos de storage compatíveis com o plug-in SnapCenter para banco de dados SAP HANA . . . 231
Mínimo de ONTAP Privileges necessário para plug-in SAP HANA . . . 232
Preparar sistemas de storage para replicação do SnapMirror e do SnapVault para bancos de dados SAP HANA . . . 235
Estratégia de backup para bancos de dados SAP HANA . . . 235
Estratégia de restauração e recuperação para bancos de dados SAP HANA . . . 239
Prepare-se para instalar o plug-in do SnapCenter para o banco de dados SAP HANA . . . 241
Fluxo de trabalho de instalação do plug-in SnapCenter para banco de dados SAP HANA . . . 241
Pré-requisitos para adicionar hosts e instalar o plug-in do SnapCenter para banco de dados SAP

HANA . . . 242
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows . . . 245
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux . . . 246
Configurar credenciais para o plug-in SnapCenter para banco de dados SAP HANA . . . 247
Configure o gMSA no Windows Server 2016 ou posterior . . . 250
Instalar o plug-in do SnapCenter para bancos de dados SAP HANA . . . 251
Configurar certificado CA . . . 257
Instale o plug-in do SnapCenter para VMware vSphere . . . 264
Implantar certificado CA . . . 265
Configure o arquivo CRL . . . 265
Preparar-se para a proteção de dados . . . 265
Pré-requisitos para usar o plug-in do SnapCenter para banco de dados SAP HANA . . . 265
Como os recursos, grupos de recursos e políticas são usados para proteger bancos de dados do SAP HANA . . . 265
Fazer backup dos recursos do SAP HANA . . . 266
Fazer backup dos recursos do SAP HANA . . . 266
Configure a chave do armazenamento de usuários HDB e o usuário do sistema operacional HDBSQL para o banco de dados SAP HANA . . . 267
Descubra recursos e prepare contentores de banco de dados multitenant para proteção de dados . . . 268
Adicione recursos manualmente ao host do plug-in . . . 271
Criar políticas de backup para bancos de dados SAP HANA . . . 272
Crie grupos de recursos e anexe políticas . . . 279
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para banco de dados SAP HANA . . . 283
Fazer backup de bancos de dados do SAP HANA . . . 285
Fazer backup de grupos de recursos . . . 292
Monitore operações de backup de bancos de dados SAP HANA . . . 292
Cancelar operações de backup para SAP HANA . . . 293
Veja os backups e clones do banco de dados SAP HANA na página topologia . . . 294
Restaure os bancos de dados do SAP HANA . . . 296
Restaure o fluxo de trabalho . . . 296
Restaure e recupere um backup de recursos adicionado manualmente . . . 297
Restaure e recupere um backup de banco de dados descoberto automaticamente . . . 301
Restaure recursos usando cmdlets do PowerShell . . . 305
Monitore as operações de restauração de bancos de dados SAP HANA . . . 307
Clonar backups de recursos do SAP HANA . . . 308
Fluxo de trabalho clone . . . 308
Clone um backup de banco de dados SAP HANA . . . 309
Monitorar operações de clone de banco de dados SAP HANA . . . 312
Divida um clone . . . 313
Exclua ou divida clones do banco de dados do SAP HANA após a atualização do SnapCenter . . . 314
Proteger bancos de dados Oracle . . . 316
Visão geral do plug-in SnapCenter para banco de dados Oracle . . . 316
O que você pode fazer com o Plug-in para Oracle Database . . . 316
Recursos do Plug-in para banco de dados Oracle . . . 316

Tipos de armazenamento suportados pelo Plug-in para Oracle Database . . . 318
Preparar sistemas de storage para replicação SnapMirror e SnapVault para plug-in para Oracle . . . 320
Mínimo de ONTAP Privileges necessário para plug-in para Oracle . . . 321
Instale o plug-in do SnapCenter para o banco de dados Oracle . . . 323
Fluxo de trabalho de instalação do plug-in SnapCenter para banco de dados Oracle . . . 323
Pré-requisitos para adicionar hosts e instalar o pacote Plug-ins para Linux ou AIX . . . 323
Adicione hosts e instale o pacote Plug-ins para Linux ou AIX usando GUI . . . 332
Maneiras alternativas de instalar o pacote Plug-ins para Linux ou AIX . . . 336
Configure o serviço SnapCenter Plug-in Loader . . . 339
Configure o certificado CA com o serviço SnapCenter Plug-in Loader (SPL) no host Linux . . . 342
Ative certificados de CA para plug-ins . . . 345
Importar dados do SnapManager para Oracle e SnapManager para SAP para SnapCenter . . . 346
Instale o plug-in do SnapCenter para VMware vSphere . . . 352
Implantar certificado CA . . . 352
Configure o arquivo CRL . . . 352
Prepare-se para proteger bancos de dados Oracle . . . 352
Faça backup de bancos de dados Oracle . . . 353
Visão geral do procedimento de backup . . . 354
Informações de configuração de backup . . . 355
Requisitos para fazer backup de um banco de dados Oracle . . . 367
Descubra os bancos de dados Oracle disponíveis para backup . . . 367
Criar políticas de backup para bancos de dados Oracle . . . 369
Crie grupos de recursos e anexe políticas para bancos de dados Oracle . . . 375
Faça backup dos recursos Oracle . . . 378
Faça backup de grupos de recursos de banco de dados Oracle . . . 380
Monitorar o backup do banco de dados Oracle . . . 381
Outras operações de backup . . . 383
Montar e desmontar backups de bancos de dados . . . 387
Montar um backup de banco de dados . . . 387
Desmontar um backup de banco de dados . . . 389
Restaurar e recuperar bancos de dados Oracle . . . 389
Restaure o fluxo de trabalho . . . 389
Definir uma estratégia de restauração e recuperação para bancos de dados Oracle . . . 389
Variáveis de ambiente predefinidas para restaurar prescrição específica e postscript . . . 394
Requisitos para restaurar um banco de dados Oracle . . . 396
Restaurar e recuperar banco de dados Oracle . . . 396
Restaure e recupere espaços de tablespaces usando recuperação ponto no tempo . . . 401
Restaurar e recuperar banco de dados conetável usando recuperação pontual . . . 403
Restaure e recupere bancos de dados Oracle usando comandos UNIX . . . 406
Monitorar operações de restauração de banco de dados Oracle . . . 406
Cancelar operações de restauração de banco de dados Oracle . . . 407
Clonar banco de dados Oracle . . . 408
Fluxo de trabalho clone . . . 408
Definir uma estratégia de clone para bancos de dados Oracle . . . 408
Variáveis de ambiente predefinidas para o prescritor específico de clone e postscript . . . 410

Requisitos para clonar um banco de dados Oracle . . . 411
Clonar um backup de banco de dados Oracle . . . 413
Clone um banco de dados conetável . . . 423
Clonar backups de bancos de dados Oracle usando comandos UNIX . . . 427
Divida um clone do banco de dados Oracle . . . 428
Clone dividido de um banco de dados conetável . . . 429
Monitorar operações de clone de banco de dados Oracle . . . 429
Atualize um clone . . . 430
Excluir clone de um banco de dados conetável . . . 431
Gerenciar volumes de aplicações . . . 432
O que são volumes de aplicações . . . 432
Adicionar volumes de aplicações . . . 432
Volumes de aplicações de backup . . . 433
Clone o backup de volume de aplicativo . . . 435
Proteja os sistemas de arquivos do Windows . . . 438
Plug-in do SnapCenter para conceitos do Microsoft Windows . . . 438
Visão geral do plug-in do SnapCenter para Microsoft Windows . . . 438
O que você pode fazer com o plug-in SnapCenter para Microsoft Windows . . . 438
Plug-in do SnapCenter para recursos do Windows . . . 438
Como o SnapCenter faz backup dos sistemas de arquivos do Windows . . . 439
Tipos de storage compatíveis com o plug-in SnapCenter para Microsoft Windows . . . 440
ONTAP Privileges mínimo necessário para o plug-in do Windows . . . 442
Preparar sistemas de storage para replicação SnapMirror e SnapVault . . . 445
Definir uma estratégia de backup para sistemas de arquivos do Windows . . . 445
Fontes e destinos de clones para sistemas de arquivos do Windows . . . 447
Instale o plug-in do SnapCenter para Microsoft Windows . . . 447
Fluxo de trabalho de instalação do plug-in SnapCenter para Microsoft Windows . . . 447
Requisitos de instalação para o plug-in SnapCenter para Microsoft Windows . . . 448
Adicione hosts e instale o plug-in do SnapCenter para Microsoft Windows . . . 452
Instale o plug-in do SnapCenter para Microsoft Windows em vários hosts remotos usando cmdlets do PowerShell . . . 456
Instale o plug-in do SnapCenter para Microsoft Windows silenciosamente a partir da linha de comando . . . 456
Monitore o status da instalação do pacote de plug-in SnapCenter . . . 458
Configure o certificado CA . . . 459
Instale o plug-in do SnapCenter para VMware vSphere . . . 462
Implantar certificado CA . . . 462
Configure o arquivo CRL . . . 462
Faça backup dos sistemas de arquivos do Windows . . . 462
Faça backup dos sistemas de arquivos do Windows . . . 462
Determinar a disponibilidade de recursos para sistemas de arquivos do Windows . . . 463
Criar políticas de backup para sistemas de arquivos do Windows . . . 464
Criar grupos de recursos para sistemas de arquivos do Windows . . . 468
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell . . . 470
Faça backup de um único recurso sob demanda para sistemas de arquivos do Windows . . . 471

Fazer backup de grupos de recursos para sistemas de arquivos do Windows . . . 475
Monitorar operações de backup . . . 476
Cancelar operações de cópia de segurança . . . 477
Veja backups e clones relacionados na página topologia . . . 478
Limpe a contagem de backup secundária usando cmdlets do PowerShell . . . 480
Restaure sistemas de arquivos do Windows . . . 481
Restaure backups do sistema de arquivos do Windows . . . 481
Restaure recursos usando cmdlets do PowerShell . . . 486
Monitorar as operações de restauração . . . 489
Cancelar operações de restauração . . . 490
Clonar sistemas de arquivos do Windows . . . 491
Clone de um backup do sistema de arquivos do Windows . . . 491
Monitorar operações de clone . . . 497
Cancelar operações de clone . . . 498
Divida um clone . . . 499
Proteja os bancos de dados do Microsoft Exchange Server . . . 501
Plug-in do SnapCenter para conceitos do Microsoft Exchange Server . . . 501
Visão geral do plug-in do SnapCenter para Microsoft Exchange Server . . . 501
O que você pode fazer com o plug-in SnapCenter para Microsoft Exchange Server . . . 501
Tipos de armazenamento suportados pelo plug-in SnapCenter para Microsoft Windows e para Microsoft Exchange Server . . . 502
ONTAP Privileges mínimo necessário para o plug-in do Exchange . . . 503
Preparar sistemas de storage para replicação SnapMirror e SnapVault . . . 506
Defina uma estratégia de backup para recursos do Exchange Server . . . 506
Defina uma estratégia de restauração para bancos de dados do Exchange . . . 509
Instale o plug-in do SnapCenter para o Microsoft Exchange Server . . . 510
Fluxo de trabalho de instalação do plug-in SnapCenter para Microsoft Exchange Server . . . 510
Pré-requisitos para adicionar hosts e instalar o plug-in do SnapCenter para Microsoft Exchange Server . . . 511
Configurar credenciais para o plug-in SnapCenter para Windows . . . 515
Configure o gMSA no Windows Server 2016 ou posterior . . . 516
Adicione hosts e instale o Plug-in para o Exchange . . . 518
Instale o plug-in para o Exchange a partir do host do servidor SnapCenter usando cmdlets do PowerShell . . . 523
Instale o plug-in SnapCenter para Exchange silenciosamente a partir da linha de comando . . . 523
Monitore o status da instalação do pacote de plug-in SnapCenter . . . 525
Configurar certificado CA . . . 526
Configure o SnapManager 7.x para Exchange e SnapCenter para coexistir . . . 529
Instale o plug-in do SnapCenter para VMware vSphere . . . 531
Implantar certificado CA . . . 531
Configure o arquivo CRL . . . 531
Preparar-se para a proteção de dados . . . 531
Pré-requisitos para usar o plug-in SnapCenter para Microsoft Exchange Server . . . 531
Como recursos, grupos de recursos e políticas são usados para proteger o Exchange Server . . . 532
Faça backup dos recursos do Exchange . . . 533

Fluxo de trabalho de backup . . . 533
Exchange banco de dados e verificação de backup . . . 534
Determine se os recursos do Exchange estão disponíveis para backup . . . 534
Criar políticas de backup para bancos de dados do Exchange Server . . . 536
Crie grupos de recursos e anexe políticas para Exchange Servers . . . 543
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para Exchange Server . . . 546
Faça backup de bancos de dados do Exchange . . . 547
Faça backup dos grupos de recursos do Exchange . . . 552
Monitorar operações de backup . . . 553
Cancelar operações de backup para o banco de dados do Exchange . . . 554
Veja backups do Exchange na página topologia . . . 555
Restaure os recursos do Exchange . . . 556
Restaure o fluxo de trabalho . . . 556
Requisitos para restaurar um banco de dados do Exchange . . . 557
Restaure bancos de dados do Exchange . . . 557
Recuperação granular de e-mails e caixa de correio . . . 562
Restaure um banco de dados do Exchange Server a partir do armazenamento secundário . . . 562
Semente novamente uma réplica passiva do nó Exchange . . . 563
Reseed uma réplica usando cmdlets do PowerShell para o banco de dados do Exchange . . . 564
Monitorar as operações de restauração . . . 564
Cancelar operações de restauração para o banco de dados do Exchange . . . 565
Proteja o IBM DB2 . . . 567
Plug-in do SnapCenter para IBM DB2 . . . 567
Visão geral do plug-in do SnapCenter para IBM DB2 . . . 567
O que você pode fazer usando o plug-in SnapCenter para IBM DB2 . . . 567
Plug-in do SnapCenter para recursos do IBM DB2 . . . 568
Tipos de storage compatíveis com o plug-in SnapCenter para IBM DB2 . . . 568
Mínimo de ONTAP Privileges necessário para o plug-in IBM DB2 . . . 569
Preparar sistemas de storage para replicação SnapMirror e SnapVault para IBM DB2 . . . 572
Estratégia de backup para IBM DB2 . . . 572
Estratégia de restauração e recuperação para IBM DB2 . . . 575
Prepare-se para instalar o plug-in do SnapCenter para IBM DB2 . . . 576
Fluxo de trabalho de instalação do plug-in SnapCenter para IBM DB2 . . . 576
Pré-requisitos para adicionar hosts e instalar o pacote Plug-ins para Windows, Linux ou AIX . . . 576
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows . . . 582
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux . . . 582
Configurar credenciais para o plug-in SnapCenter para IBM DB2 . . . 583
Configure o gMSA no Windows Server 2016 ou posterior . . . 586
Instale o plug-in do SnapCenter para IBM DB2 . . . 587
Configurar certificado CA . . . 593
Preparar-se para a proteção de dados . . . 601
Pré-requisitos para usar o plug-in SnapCenter para IBM DB2 . . . 601
Como recursos, grupos de recursos e políticas são usados para proteger o IBM DB2 . . . 601
Faça backup dos recursos do IBM DB2 . . . 602

Faça backup dos recursos do IBM DB2 . . . 602
Descubra os bancos de dados automaticamente . . . 604
Adicione recursos manualmente ao host do plug-in . . . 604
Criar políticas de backup para o IBM DB2 . . . 606
Crie grupos de recursos e anexe políticas . . . 607
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para IBM DB2 . . . 611
Faça backup de bancos de dados DB2 . . . 613
Fazer backup de grupos de recursos . . . 619
Monitorar operações de backup do IBM DB2 . . . 620
Cancelar operações de backup para IBM DB2 . . . 621
Veja os backups e clones do IBM DB2 na página topologia . . . 622
Restaure o IBM DB2 . . . 623
Restaure o fluxo de trabalho . . . 623
Restaurar um backup de recursos adicionado manualmente . . . 624
Restaure e recupere um backup de banco de dados descoberto automaticamente . . . 628
Monitorar operações de restauração do IBM DB2 . . . 629
Clonar backups de recursos do IBM DB2 . . . 630
Fluxo de trabalho clone . . . 630
Clonar um backup do IBM DB2 . . . 631
Monitorar operações de clone do IBM DB2 . . . 638
Divida um clone . . . 639
Exclua ou divida clones do banco de dados IBM DB2 após a atualização do SnapCenter . . . 640
Proteja o PostgreSQL . . . 642
Plug-in SnapCenter para PostgreSQL . . . 642
Visão geral do plug-in do SnapCenter para PostgreSQL . . . 642
O que você pode fazer usando o plug-in SnapCenter para PostgreSQL . . . 642
Plug-in do SnapCenter para recursos PostgreSQL . . . 642
Tipos de armazenamento suportados pelo plug-in SnapCenter para PostgreSQL . . . 643
Mínimo de ONTAP Privileges necessário para o plug-in PostgreSQL . . . 644
Prepare sistemas de storage para replicação SnapMirror e SnapVault para PostgreSQL . . . 647
Estratégia de backup para PostgreSQL . . . 647
Estratégia de restauração e recuperação para PostgreSQL . . . 650
Prepare-se para instalar o plug-in SnapCenter para PostgreSQL . . . 651
Fluxo de trabalho de instalação do plug-in SnapCenter para PostgreSQL . . . 651
Pré-requisitos para adicionar hosts e instalar o plug-in SnapCenter para PostgreSQL . . . 652
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows . . . 655
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux . . . 656
Configure credenciais para o plug-in SnapCenter para PostgreSQL . . . 657
Configure o gMSA no Windows Server 2016 ou posterior . . . 660
Instale o plug-in SnapCenter para PostgreSQL . . . 661
Configurar certificado CA . . . 667
Preparar-se para a proteção de dados . . . 675
Pré-requisitos para usar o plug-in SnapCenter para PostgreSQL . . . 675
Como recursos, grupos de recursos e políticas são usados para proteger o PostgreSQL . . . 675

Faça backup dos recursos do PostgreSQL . . . 676
Faça backup dos recursos do PostgreSQL . . . 676
Descobrir os clusters automaticamente . . . 678
Adicione recursos manualmente ao host do plug-in . . . 678
Crie políticas de backup para PostgreSQL . . . 680
Crie grupos de recursos e anexe políticas . . . 682
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para PostgreSQL . . . 685
Faça backup do PostgreSQL . . . 687
Fazer backup de grupos de recursos . . . 692
Monitore as operações de backup do PostgreSQL . . . 693
Cancelar operações de backup para PostgreSQL . . . 694
Veja backups e clones do PostgreSQL na página topologia . . . 695
Restaure o PostgreSQL . . . 696
Restaure o fluxo de trabalho . . . 696
Restaure e recupere um backup de recursos adicionado manualmente . . . 697
Restaure e recupere um backup de cluster descoberto automaticamente . . . 701
Restaure recursos usando cmdlets do PowerShell . . . 703
Monitore as operações de restauração do PostgreSQL . . . 706
Clonar backups de recursos do PostgreSQL . . . 707
Fluxo de trabalho clone . . . 707
Clonar um backup PostgreSQL . . . 708
Monitore as operações de clone do PostgreSQL . . . 711
Divida um clone . . . 712
Exclua ou divida clones do cluster do PostgreSQL após a atualização do SnapCenter . . . 713
Proteja o MySQL . . . 715
Plug-in SnapCenter para MySQL . . . 715
Visão geral do plug-in SnapCenter para MySQL . . . 715
O que você pode fazer usando o plug-in SnapCenter para MySQL . . . 715
Plug-in do SnapCenter para recursos MySQL . . . 715
Tipos de armazenamento suportados pelo plug-in SnapCenter para MySQL . . . 716
ONTAP Privileges mínimo necessário para o plug-in MySQL . . . 717
Preparar sistemas de storage para replicação SnapMirror e SnapVault para MySQL . . . 720
Estratégia de backup para MySQL . . . 720
Estratégia de restauração e recuperação para MySQL . . . 723
Prepare-se para instalar o plug-in SnapCenter para MySQL . . . 724
Fluxo de trabalho de instalação do plug-in SnapCenter para MySQL . . . 724
Pré-requisitos para adicionar hosts e instalar o plug-in SnapCenter para MySQL . . . 724
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows . . . 728
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux . . . 728
Configure credenciais para o plug-in SnapCenter para MySQL . . . 729
Instale o plug-in SnapCenter para MySQL . . . 732
Configurar certificado CA . . . 737
Preparar-se para a proteção de dados . . . 745
Pré-requisitos para usar o plug-in SnapCenter para MySQL . . . 745

Como recursos, grupos de recursos e políticas são usados para proteger o MySQL . . . 745
Faça backup de recursos MySQL . . . 746
Faça backup de recursos MySQL . . . 746
Descubra os bancos de dados automaticamente . . . 748
Adicione recursos manualmente ao host do plug-in . . . 748
Criar políticas de backup para MySQL . . . 749
Crie grupos de recursos e anexe políticas . . . 751
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para MySQL . . . 755
Faça backup do MySQL . . . 757
Fazer backup de grupos de recursos . . . 762
Monitorar operações de backup do MySQL . . . 763
Cancelar operações de backup para MySQL . . . 764
Veja backups e clones do MySQL na página topologia . . . 765
Restaure o MySQL . . . 766
Restaure o fluxo de trabalho . . . 766
Restaure e recupere um backup de recursos adicionado manualmente . . . 767
Restaure e recupere um backup de banco de dados descoberto automaticamente . . . 771
Restaure recursos usando cmdlets do PowerShell . . . 773
Monitorar operações de restauração do MySQL . . . 775
Clonar backups de recursos MySQL . . . 776
Fluxo de trabalho clone . . . 776
Clonar um backup MySQL . . . 777
Monitorar operações de clone do MySQL . . . 780
Divida um clone . . . 781
Excluir ou dividir clones do banco de dados MySQL após a atualização do SnapCenter . . . 782
Proteja aplicativos usando plug-ins compatíveis com NetApp . . . 783
Plug-ins compatíveis com NetApp . . . 783
Visão geral dos plug-ins compatíveis com NetApp . . . 783
O que você pode fazer com os plug-ins compatíveis com o NetApp . . . 783
Recursos de plug-ins compatíveis com NetApp . . . 784
Tipos de storage compatíveis com plug-ins compatíveis com NetApp . . . 785
Mínimo de ONTAP Privileges necessário para o plug-in compatível com NetApp . . . 785
Preparar sistemas de storage para a replicação do SnapMirror e do SnapVault para plug-ins compatíveis com NetApp . . . 787
Defina uma estratégia de backup . . . 788
Estratégia de backup para plug-ins compatíveis com NetApp . . . 789
Tipos de estratégias de restauração compatíveis com recursos de plug-in compatíveis com NetApp adicionados manualmente . . . 789
Prepare-se para instalar plug-ins compatíveis com NetApp . . . 790
Fluxo de trabalho de instalação de plug-ins compatíveis com SnapCenter NetApp . . . 790
Pré-requisitos para adicionar hosts e instalar o pacote Plug-ins para Windows, Linux ou AIX . . . 790
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Windows . . . 795
Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux e AIX . . . 796
Configurar credenciais para plug-ins compatíveis com NetApp . . . 797

Configure o gMSA no Windows Server 2016 ou posterior . . . 799
Instale os plug-ins suportados pelo NetApp . . . 800
Configurar certificado CA . . . 807
Preparar-se para a proteção de dados . . . 814
Pré-requisitos para usar os plug-ins suportados pelo NetApp . . . 814
Como os recursos, grupos de recursos e políticas são usados para proteger os recursos de plug-in compatíveis com o NetApp . . . 815
Fazer backup de recursos de plug-ins compatíveis com NetApp . . . 816
Fazer backup de recursos de plug-ins compatíveis com NetApp . . . 816
Adicione recursos aos plug-ins compatíveis com NetApp . . . 816
Criar políticas para recursos de plug-in compatíveis com o NetApp . . . 821
Crie grupos de recursos e anexe políticas . . . 825
Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell . . . 829
Fazer backup de recursos de plug-ins compatíveis com NetApp individuais . . . 830
Fazer backup de grupos de recursos de plug-in compatíveis com o NetApp . . . 835
Monitorar as operações de backup de recursos de plug-in compatíveis com NetApp . . . 836
Cancelar operações de backup para plug-ins compatíveis com NetApp . . . 837
Veja os backups e clones relacionados a recursos de plug-ins compatíveis com o NetApp na página topologia . . . 838
Restaure os recursos de plug-ins compatíveis com o NetApp . . . 839
Restaure os recursos de plug-in compatíveis com o NetApp . . . 839
Restaurar um backup de recursos . . . 840
Monitorar as operações de restauração de recursos de plug-in compatíveis com o NetApp . . . 844
Clone NetApp compatível com backups de recursos de plug-ins . . . 845
Clone NetApp compatível com backups de recursos de plug-ins . . . 845
Clone de um backup . . . 846
Monitorar as operações de clone de recurso de plug-in compatíveis com o NetApp . . . 852
Proteja sistemas de arquivos Unix . . . 854
O que você pode fazer com o plug-in SnapCenter para sistemas de arquivos Unix . . . 854
Configurações compatíveis . . . 854
Limitações . . . 855
Instale o plug-in SnapCenter para sistemas de arquivos Unix . . . 855
Pré-requisitos para adicionar hosts e instalar o pacote Plug-ins para Linux . . . 855
Adicione hosts e instale o pacote Plug-ins para Linux usando GUI . . . 856
Configure o serviço SnapCenter Plug-in Loader . . . 859
Configure o certificado CA com o serviço SnapCenter Plug-in Loader (SPL) no host Linux . . . 862
Ative certificados de CA para plug-ins . . . 865
Instale o plug-in do SnapCenter para VMware vSphere . . . 866
Implantar certificado CA . . . 866
Configure o arquivo CRL . . . 866
Prepare-se para proteger sistemas de arquivos Unix . . . 866
Faça backup de sistemas de arquivos Unix . . . 867
Descubra os sistemas de arquivos UNIX disponíveis para backup . . . 867
Crie políticas de backup para sistemas de arquivos Unix . . . 867
Crie grupos de recursos e anexe políticas para sistemas de arquivos Unix . . . 870

Faça backup de sistemas de arquivos Unix . . . 873
Fazer backup de grupos de recursos de sistemas de arquivos Unix . . . 874
Monitorar backup de sistemas de arquivos Unix . . . 875
Veja sistemas de arquivos Unix protegidos na página topologia . . . 876
Restaurar e recuperar sistemas de arquivos Unix . . . 878
Restaure sistemas de arquivos Unix . . . 878
Monitorar operações de restauração de sistemas de arquivos Unix . . . 879
Clonar sistemas de arquivos Unix . . . 880
Clone backup do sistema de arquivos Unix . . . 880
Divida um clone . . . 881
Monitorar operações de clones de sistemas de arquivos Unix . . . 883
Proteja aplicativos em execução no Azure NetApp Files . . . 884
Proteja aplicativos em execução no Azure NetApp Files . . . 884
Limitações . . . 884
Instale o SnapCenter e crie credenciais . . . 884
Instale o SnapCenter na Máquina Virtual do Azure . . . 884
Crie a credencial do Azure no SnapCenter . . . 886
Configure a conta de armazenamento do Azure . . . 886
Crie a credencial para adicionar o host do plug-in . . . 887
Proteger bancos de dados SAP HANA . . . 887
Adicione hosts e instale o plug-in do SnapCenter para banco de dados SAP HANA . . . 888
Adicionar banco de dados SAP HANA . . . 888
Criar políticas de backup para bancos de dados SAP HANA . . . 889
Crie grupos de recursos e anexe políticas de backup do SAP HANA . . . 890
Fazer backup de bancos de dados SAP HANA executados no Azure NetApp Files . . . 890
Fazer backup de grupos de recursos do SAP HANA . . . 892
Restaure e recupere bancos de dados do SAP HANA . . . 892
Clone o backup do banco de dados SAP HANA . . . 893
Proteja bancos de dados Microsoft SQL Server . . . 894
Adicione hosts e instale o plug-in do SnapCenter para o banco de dados SQL Server . . . 894
Criar políticas de backup para bancos de dados do SQL Server . . . 895
Crie grupos de recursos e anexe políticas de backup SQL . . . 896
Faça backup de bancos de dados do SQL Server em execução no Azure NetApp Files . . . 897
Fazer backup de grupos de recursos do SQL Server . . . 898
Restaurar e recuperar bancos de dados do SQL Server . . . 899
Clone backup do banco de dados SQL Server . . . 900
Proteger bancos de dados Oracle . . . 902
Adicione hosts e instale o plug-in do SnapCenter para o banco de dados Oracle . . . 902
Criar políticas de backup para bancos de dados Oracle . . . 902
Crie grupos de recursos e anexe políticas de backup Oracle . . . 903
Faça backup de bancos de dados Oracle em execução no Azure NetApp Files . . . 904
Fazer backup de grupos de recursos Oracle . . . 905
Restaurar e recuperar bancos de dados Oracle . . . 905
Clone backup de banco de dados Oracle . . . 908
Gerencie o servidor SnapCenter e os plug-ins . . . 911

Visualização do painel . . . 911
Visão geral do painel de instrumentos . . . 911
Como visualizar informações no painel de instrumentos . . . 915
Solicitar relatórios de status dos trabalhos a partir do painel de controle . . . 915
Solicite relatórios sobre o status da proteção a partir do painel de controle . . . 916
Gerenciar RBAC . . . 916
Modificar uma função . . . 916
Modificar usuários e grupos . . . 917
Gerenciar hosts . . . 917
Atualize as informações da máquina virtual . . . 919
Modificar hosts de plug-in . . . 919
Inicie ou reinicie os serviços de plug-in . . . 920
Suspender programações para manutenção do host . . . 921
Operações suportadas a partir da página recursos . . . 921
Gerenciar políticas . . . 922
Modificar políticas . . . 922
Desanexe políticas . . . 923
Eliminar políticas . . . 924
Gerenciar grupos de recursos . . . 924
Parar e retomar as operações em grupos de recursos . . . 925
Eliminar grupos de recursos . . . 925
Gerenciar backups . . . 925
Renomear backups . . . 925
Eliminar cópias de segurança . . . 926
Remova a proteção . . . 927
Excluir clones . . . 927
Monitore trabalhos, horários, eventos e logs . . . 928
Monitorizar trabalhos . . . 928
Monitorar programações . . . 929
Monitorar eventos . . . 929
Monitorizar registos . . . 930
Remover trabalhos e registos do SnapCenter . . . 931
Visão geral dos recursos de relatórios do SnapCenter . . . 931
Acesse relatórios . . . 933
Filtre seu relatório . . . 933
Exportar ou imprimir relatórios . . . 934
Defina o servidor SMTP para notificações por e-mail . . . 934
Configure a opção para enviar relatórios por e-mail . . . 934
Gerenciar o repositório do servidor SnapCenter . . . 935
Pré-requisitos para proteger o repositório SnapCenter . . . 935
Faça backup do repositório do SnapCenter . . . 935
Veja os backups do repositório SnapCenter . . . 936
Restaure o repositório de banco de dados do SnapCenter . . . 936
Migrar o repositório SnapCenter . . . 937
Redefina a senha do repositório do SnapCenter . . . 937

Gerencie recursos de domínios não confiáveis . . . 938
Modifique domínios não confiáveis . . . 938
Anular o registo de domínios não fidedignos do ative Directory . . . 939
Gerencie o sistema de storage . . . 939
Modificar a configuração do sistema de storage . . . 940
Elimine o sistema de armazenamento . . . 942
Gerir a recolha de dados EMS . . . 943
Parar a recolha de dados EMS . . . 943
Inicie a recolha de dados EMS . . . 943
Alterar o cronograma de coleta de dados do EMS e o SVM de destino . . . 943
Monitorize o estado da recolha de dados EMS . . . 944
Atualize o servidor SnapCenter e os plug-ins . . . 945
Configure o SnapCenter para verificar se há atualizações disponíveis . . . 945
Atualizar fluxo de trabalho . . . 945
Caminhos de atualização suportados . . . 945
Atualize o servidor SnapCenter no host Windows . . . 946
Atualize o servidor SnapCenter no host Linux . . . 948
Atualize seus pacotes de plug-in . . . 949
Atualização técnica . . . 952
Atualização técnica do host do servidor SnapCenter . . . 952
Atualização técnica de um nó no cluster F5 . . . 953
Desativação do antigo host do servidor SnapCenter . . . 953
Reverter para o antigo host do servidor SnapCenter . . . 953
Recuperação de desastres . . . 953
Atualização técnica dos hosts de plug-in do SnapCenter . . . 955
Atualização técnica do sistema de storage . . . 957
Atualize os backups do armazenamento primário . . . 958
Atualize os backups do armazenamento secundário . . . 960
Desinstale o servidor SnapCenter e os plug-ins . . . 962
Desinstalar pacotes de plug-in do SnapCenter . . . 962
Pré-requisitos para remover um host . . . 962
Remova um host . . . 963
Desinstale os plug-ins usando a GUI do SnapCenter . . . 963
Desinstale os plug-ins do Windows usando o cmdlet PowerShell . . . 964
Desinstale os plug-ins localmente em um host . . . 965
Desinstale o pacote de plug-ins para Linux ou AIX usando CLI . . . 965
Desinstale o servidor SnapCenter no host Windows . . . 966
Desinstale o servidor SnapCenter no host Linux . . . 966
Automatize com o uso de APIS REST . . . 968
Visão geral das APIs REST . . . 968
Como acessar a API REST do SnapCenter nativamente . . . 968
Base de serviços web REST . . . 968
Recursos e representação do Estado . . . 968
Pontos de extremidade URI . . . 969
Mensagens HTTP . . . 969

Formatação JSON . . . 969
Caraterísticas operacionais básicas . . . 969
Transação de API de solicitação e resposta . . . 969
Suporte para operações CRUD . . . 969
Identificadores de objeto . . . 970
Instâncias e coleções de objetos . . . 970
Operações síncronas e assíncronas . . . 970
Segurança . . . 970
Variáveis de entrada que controlam uma solicitação de API . . . 971
Métodos HTTP . . . 971
Cabeçalhos de solicitação . . . 971
Corpo do pedido . . . 971
Filtrando objetos . . . 972
Solicitando campos de objeto específicos . . . 972
Ordenar objetos no conjunto de saída . . . 973
Paginação ao recuperar objetos em uma coleção . . . 973
Propriedades de tamanho . . . 974
Interpretação de uma resposta API . . . 974
Código de status HTTP . . . 974
Cabeçalhos de resposta . . . 975
Corpo de resposta . . . 975
Erros . . . 976
APIs REST compatíveis com servidor SnapCenter e plug-ins . . . 977
Auth . . . 977
Domínios . . . 977
Trabalhos . . . 977
Definições . . . 977
Hosts . . . 978
Recursos . . . 978
Backups . . . 980
Clones . . . 980
Divisão de clones . . . 980
Grupos de recursos . . . 980
Políticas . . . 981
Armazenamento . . . 981
Partilhar . . . 981
Plugins . . . 982
Relatórios . . . 983
Alertas . . . 983
RBAC . . . 983
Configuração . . . 983
CertificateSettings . . . 983
Repositório . . . 984
Versão . . . 984
Como acessar APIs REST usando a página da Web da API Swagger . . . 984

Comece a usar a API REST . . . 985
Olá mundo . . . 985
Avisos legais . . . 986
Direitos de autor . . . 986
Marcas comerciais . . . 986
Patentes . . . 986
Política de privacidade . . . 986
Código aberto . . . 986

Documentação do software SnapCenter

Notas de lançamento

Notas de lançamento

Saiba mais sobre os novos e aprimorados recursos disponíveis no SnapCenter 6,0 e 6,0.1.

Para obter uma lista completa de novos recursos e aprimoramentos, consulte "Novidades do SnapCenter 6.0.1" e "Novidades do SnapCenter 6,0".

Para obter detalhes sobre problemas conhecidos, limitações, problemas corrigidos e comandos novos e alterados, consulte o "Notas de versão do software SnapCenter 6,0 e 6.0.1". Você deve entrar com sua conta do NetApp ou criar uma conta para acessar as Notas de versão.

Caminhos de atualização compatíveis para o SnapCenter

O caminho de atualização ajuda você a entender a partir de 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 do servidor SnapCenter…	Você pode atualizar diretamente o servidor SnapCenter para…	Versões de plug-in suportadas
4,9	5,0	• 4,9 • 5,0
	6,0	• 6,0
5,0	6,0	• 5,0 • 6,0
	6.0.1	• 6.0.1
6,0	6.0.1	• 6,0 • 6.0.1

Por exemplo, se você estiver no SnapCenter versão 4,9 e quiser atualizar para 6,0.1, primeiro você deve atualizar para 5,0 e, em seguida, fazer uma atualização contínua para 6,0.1.

Para obter informações sobre como atualizar o plug-in do SnapCenter para VMware vSphere, "Atualize o plug-in do SnapCenter para o VMware vSphere" consulte .

Conceitos

Visão geral do SnapCenter

O software SnapCenter é uma plataforma simples, centralizada e dimensionável que fornece proteção de dados consistente com aplicações para aplicações, bancos de dados, sistemas de arquivos host e VMs em execução nos sistemas ONTAP em qualquer lugar na nuvem híbrida.

O SnapCenter utiliza as tecnologias NetApp Snapshot, SnapRestore, FlexClone, SnapMirror e SnapVault para oferecer o seguinte:

- Backups rápidos, com uso eficiente de espaço, consistentes com aplicações e baseados em disco
- Restauração rápida e granular, e recuperação consistente com aplicações
- Clonagem rápida e com uso eficiente de espaço

O SnapCenter inclui o servidor SnapCenter e plug-ins leves individuais. É possível automatizar a implantação de plug-ins para hosts remotos de aplicações, agendar operações de backup, verificação e clone e monitorar todas as operações de proteção de dados.

O SnapCenter pode ser implantado das seguintes maneiras:

- No local para proteger o seguinte:
  - Dados em sistemas primários ONTAP FAS, AFF ou All SAN Array (ASA) e replicados para sistemas secundários ONTAP FAS, AFF ou ASA
  - Dados em sistemas primários ONTAP Select
  - Dados em sistemas primários e secundários ONTAP FAS, AFF ou ASA e protegidos no storage de objetos StorageGRID local
- No local em uma nuvem híbrida para proteger o seguinte:
  - Dados em sistemas primários ONTAP FAS, AFF ou ASA e replicados para Cloud Volumes ONTAP
  - Dados que estão em sistemas primários e secundários ONTAP FAS, AFF ou ASA e protegidos para armazenamento de objetos e arquivos na nuvem usando integração de backup e recuperação do NetApp
- Em uma nuvem pública para proteger o seguinte:
  - Dados em sistemas primários Cloud Volumes ONTAP (anteriormente ONTAP Cloud)
  - Dados que estão no Amazon FSX for ONTAP
  - Dados em Azure NetApp Files primário (Oracle, Microsoft SQL e SAP HANA)

O SnapCenter inclui os seguintes recursos principais:

- Proteção de dados centralizada e consistente com aplicações

  A proteção de dados é compatível com bancos de dados Microsoft Exchange Server, Microsoft SQL Server, Oracle em Linux ou AIX, banco de dados SAP HANA, IBM DB2, PostgreSQL, MySQL e Windows Host em execução em sistemas ONTAP. O SnapCenter também oferece suporte à proteção de aplicativos como MongoDB, Storage, MaxDB, Sybase ASE e ORASCPM.

- Backups baseados em políticas

  Os backups baseados em políticas utilizam a tecnologia NetApp Snapshot para criar backups rápidos, com uso eficiente de espaço, consistentes com aplicações e baseados em disco. Como opção, você pode automatizar a proteção desses backups para um storage secundário por meio de atualizações dos relacionamentos de proteção existentes.

- Backups para vários recursos

  É possível fazer backup de vários recursos (aplicações, 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 granulares e rápidas de backups e recuperação baseada em tempo e consistente com aplicações. Você pode restaurar a partir de qualquer destino na nuvem híbrida.

- Clonagem

  O SnapCenter fornece clonagem rápida, com uso eficiente de espaço e consistente com aplicações, o que possibilita o desenvolvimento acelerado de software. Você pode clonar em qualquer destino na nuvem híbrida.

- Interface gráfica do usuário (GUI) de gerenciamento de usuário único

  A GUI do SnapCenter fornece uma interface única e única para gerenciar backups e clones de um recurso em qualquer destino na nuvem híbrida.

- APIs REST, cmdlets do Windows, comandos UNIX

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

  Para obter mais informações sobre APIs REST, "Visão geral da API REST"consulte .

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

  Para obter mais informações sobre comandos UNIX, "Guia de Referência de comandos do software SnapCenter"consulte .

- Dashboard e relatórios centralizados de proteção de dados
- Controle de acesso baseado em função (RBAC) para segurança e delegação.
- Banco de dados de repositório com alta disponibilidade

  O SnapCenter fornece um banco de dados de repositório integrado com alta disponibilidade para armazenar todos os metadados de backup.

- Instalação automática de plug-ins por push

  Você pode automatizar um envio remoto de plug-ins do SnapCenter do host do servidor SnapCenter para os hosts de aplicativos.

- Alta disponibilidade

A alta disponibilidade para SnapCenter é configurada usando o balanceador de carga externo (F5). Até dois nós são suportados no mesmo data center.

- Recuperação de desastres (DR)

  Você pode recuperar o servidor SnapCenter em caso de desastres como corrupção de recursos ou falha do servidor.

- SnapLock

  O SnapLock é uma solução de conformidade de alto desempenho para organizações que usam storage WORM (uma gravação, muitas leituras) para reter arquivos de forma não modificada para fins regulatórios e de governança.

  Para obter mais informações sobre o SnapLock, consulte "O que é SnapLock"

- SnapMirror ative Sync (lançado inicialmente como SnapMirror Business Continuity [SM-BC])

  O SnapMirror active Sync permite que os serviços empresariais continuem operando mesmo em uma falha completa do local, com suporte ao failover de aplicações de forma transparente, usando uma cópia secundária. Nem a intervenção manual nem o script adicional são necessários para acionar um failover com a sincronização ativa do SnapMirror.

  Os plug-ins suportados para esse recurso são plug-in SnapCenter para 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 e plug-in SnapCenter para Unix.

  > Para suportar a proximidade do iniciador do host no SnapCenter, seu valor, origem ou destino deve ser definido no ONTAP.

  A funcionalidade de sincronização ativa do SnapMirror não é suportada no SnapCenter:

  - Se você converter as cargas de trabalho de sincronização ativa assimétrica do SnapMirror existentes para simétricas alterando a política nas relações 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 nas relações de sincronização ativa do SnapMirror de *automatedfailover* para *automatedfailoverduplex* no ONTAP, o mesmo não é suportado no SnapCenter.

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

  Para a sincronização ativa do SnapMirror, verifique se você atendeu aos vários requisitos de configuração de hardware, software e sistema. Para obter mais informações, consulte "Pré-requisitos"

- Espelhamento síncrono

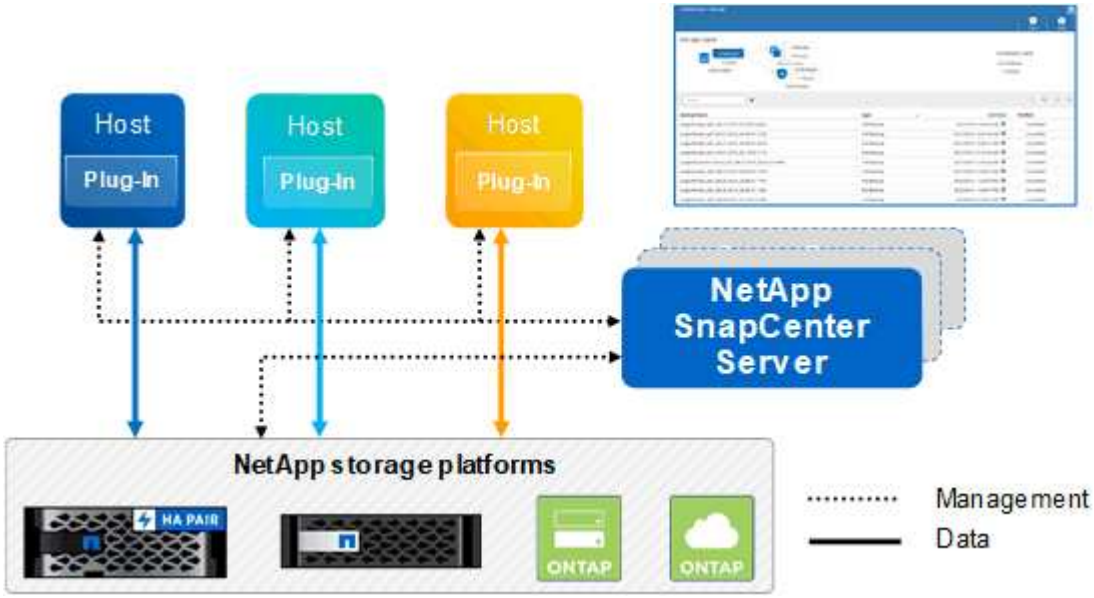
  O recurso de espelhamento síncrono oferece replicação de dados on-line em tempo real entre storage arrays em uma distância remota.

  Para obter mais informações sobre o espelho de sincronização, consulte "Visão geral do espelhamento síncrono"

Arquitetura da SnapCenter

A plataforma SnapCenter é baseada em uma arquitetura de vários níveis que inclui um servidor de gerenciamento centralizado (servidor SnapCenter) e um host de plug-in SnapCenter.

O SnapCenter é compatível com data center multisite. O servidor SnapCenter e o host do plug-in podem estar em diferentes locais geográficos.



Componentes do SnapCenter

O SnapCenter consiste nos plug-ins do servidor SnapCenter e do SnapCenter. Você deve instalar apenas os plug-ins apropriados para os dados que deseja proteger.

- Servidor SnapCenter
- Pacote de plug-ins do SnapCenter para Windows, que inclui os seguintes plug-ins:
  - Plug-in do SnapCenter para Microsoft SQL Server
  - Plug-in do SnapCenter para Microsoft Windows
  - Plug-in do SnapCenter para Microsoft Exchange Server
  - Plug-in do SnapCenter para banco de dados SAP HANA
  - Plug-in do SnapCenter para IBM DB2
  - Plug-in SnapCenter para PostgreSQL
  - Plug-in SnapCenter para MySQL
  - Plug-in do SnapCenter para MongoDB
  - Plug-in SnapCenter para ORASCPM (aplicações Oracle)
  - Plug-in do SnapCenter para SAP ASE
  - Plug-in do SnapCenter para SAP MaxDB
  - Plug-in do SnapCenter para plug-in de storage
- Pacote de plug-ins do SnapCenter para Linux, que inclui os seguintes plug-ins:
  - Plug-in SnapCenter para banco de dados Oracle

    - Plug-in do SnapCenter para banco de dados SAP HANA
    - Plug-in do SnapCenter para sistemas de arquivos UNIX
    - Plug-in do SnapCenter para IBM DB2
    - Plug-in SnapCenter para PostgreSQL
    - Plug-in SnapCenter para MySQL
    - Plug-in do SnapCenter para MongoDB
    - Plug-in SnapCenter para ORASCPM (aplicações Oracle)
    - Plug-in do SnapCenter para SAP ASE
    - Plug-in do SnapCenter para SAP MaxDB
    - Plug-in do SnapCenter para plug-in de storage
- Pacote de plug-ins do SnapCenter para AIX, que inclui os seguintes plug-ins:
    - Plug-in SnapCenter para banco de dados Oracle
    - Plug-in do SnapCenter para sistemas de arquivos UNIX
    - Plug-in do SnapCenter para IBM DB2

O plug-in do SnapCenter para VMware vSphere, antigo agente de dados da NetApp, é um dispositivo virtual autônomo que suporta operações de proteção de dados da SnapCenter em bancos de dados virtualizados e sistemas de arquivos.

Servidor SnapCenter

O servidor SnapCenter inclui um servidor da Web, uma interface de usuário centralizada baseada em HTML5, cmdlets do PowerShell, APIs REST e o repositório SnapCenter.

Servidor SnapCenter suporta Microsoft Windows e Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5)

Se você estiver usando o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX, as programações são executadas centralmente usando o agendador de quartzo.

- Para o plug-in do SnapCenter para banco de dados Oracle, o agente host que é executado no host do servidor SnapCenter se comunica com o SnapCenter Plug-in Loader (SPL) que é executado no host Linux ou AIX para executar diferentes operações de proteção de dados.
- Para o SnapCenter Plug-in para banco de dados SAP HANA, o SnapCenter Server se comunica com o plug-in por meio do agente SCCore que é executado no host.

O servidor SnapCenter e os plug-ins se comunicam com o agente host usando HTTPS. As informações sobre as operações do SnapCenter são armazenadas no repositório do SnapCenter.

> O SnapCenter oferece suporte a namespace disjoint para hosts do Windows. Se você enfrentar problemas ao usar o namespace disjoint, "O SnapCenter não consegue descobrir recursos ao usar namespace disjoint" consulte .

Você deve executar os seguintes comandos para saber o status dos componentes do SnapCenter em execução no host Linux:

- `systemctl status snapmanagerweb`
- `systemctl status scheduler`

- `systemctl status smcore`
- `systemctl status nginx`
- `systemctl status rabbitmq-server`

Plug-ins do SnapCenter

Cada plug-in do SnapCenter é compatível com ambientes, bancos de dados e aplicações específicos.

Nome do plug-in	Incluído no pacote de instalação	Requer outros plug-ins	Instalado no host	Plataforma suportada
Plug-in para SQL Server	Pacote de plug-ins para Windows	Plug-in para Windows	Host do SQL Server	Windows
Plug-in para Windows	Pacote de plug-ins para Windows		Host Windows	Windows
Plug-in para Exchange	Pacote de plug-ins para Windows	Plug-in para Windows	Host do Exchange Server	Windows
Plug-in 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
Plug-in 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 cliente HDBSQL	Linux ou Windows
Plug-in 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	DB2 host	Linux ou Windows
Plug-in para PostgreSQL	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou Plug-in para Windows	PostgreSQL host	Linux ou Windows
Plug-in para MySQL	Pacote de plug-ins para Linux e pacote de plug-ins para Windows	Plug-in para UNIX ou Plug-in para Windows	Db2MySQL host	Linux ou Windows
Plug-in 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

Nome do plug-in	Incluído no pacote de instalação	Requer outros plug-ins	Instalado no host	Plataforma suportada
Plug-in 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 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 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 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 storage	Linux ou Windows

O plug-in do SnapCenter para VMware vSphere é compatível com operações de backup e restauração consistentes com VM e falhas para máquinas virtuais (VMs), armazenamentos de dados e discos de máquinas virtuais (VMDKs), além de oferecer suporte aos plug-ins específicos da aplicação SnapCenter para proteger operações de backup e restauração consistentes com aplicações para bancos de dados e sistemas de arquivos virtualizados.

Para usuários do SnapCenter 4.1.1, a documentação do plug-in do SnapCenter para VMware vSphere 4.1.1 tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos. Para usuários do SnapCenter 4,2.x, o Agente de dados do NetApp 1,0 e 1,0.1, a documentação tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in do SnapCenter para VMware vSphere fornecido pelo dispositivo virtual NetApp Data Broker baseado em Linux (formato Open Virtual Appliance). Para usuários que usam o SnapCenter 4,3 ou posterior, o "Plug-in do SnapCenter para documentação do VMware vSphere" tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in SnapCenter baseado em Linux para o dispositivo virtual VMware vSphere (formato Open Virtual Appliance).

Plug-in do SnapCenter para recursos do Microsoft SQL Server

- Automatiza operações de backup, restauração e clone com reconhecimento de aplicações para bancos de dados Microsoft SQL Server em seu ambiente SnapCenter.
- Suporta bancos de dados Microsoft SQL Server em VMDK e LUNs de mapeamento de dispositivo bruto (RDM) quando você implementa o plug-in SnapCenter para VMware vSphere e Registra o plug-in com o SnapCenter
- É compatível apenas com o provisionamento de compartilhamentos SMB. Não é fornecido suporte para fazer backup de bancos de dados SQL Server em compartilhamentos SMB.
- Suporta a importação de backups do SnapManager para Microsoft SQL Server para SnapCenter.

Plug-in do SnapCenter para recursos do Microsoft Windows

- Habilita a proteção de dados com reconhecimento de aplicativos para outros plug-ins que estão sendo executados em hosts do Windows em seu ambiente SnapCenter
- Automatiza operações de backup, restauração e clone com reconhecimento de aplicações para sistemas de arquivos da Microsoft em seu ambiente SnapCenter
- É compatível com o provisionamento de storage, a consistência Snapshot e a exigência de espaço para hosts do Windows

> O Plug-in para Windows provisiona compartilhamentos SMB e sistemas de arquivos do Windows em LUNs físicos e RDM, mas não suporta operações de backup para sistemas de arquivos do Windows em compartilhamentos SMB.

Plug-in do SnapCenter para recursos do Microsoft Exchange Server

- Automatiza as operações de backup e restauração com reconhecimento de aplicativos para bancos de dados do Microsoft Exchange Server e grupos de disponibilidade de banco de dados (DAGs) em seu ambiente SnapCenter
- Suporta servidores Exchange virtualizados em LUNs RDM quando você implementa o plug-in SnapCenter para VMware vSphere e Registra o plug-in com o SnapCenter

Plug-in do SnapCenter para recursos de banco de dados Oracle

- Automatiza operações de backup, restauração, recuperação, verificação, montagem, desmontagem e clone com reconhecimento de aplicações para bancos de dados Oracle em seu ambiente SnapCenter
- Suporta bancos de dados Oracle para SAP, no entanto, a integração SAP BR*Tools não é fornecida

Plug-in do SnapCenter para recursos UNIX

- Permite que o Plug-in para Oracle Database execute operações de proteção de dados em bancos de dados Oracle, manipulando a pilha de armazenamento de host subjacente em sistemas Linux ou AIX
- Dá suporte aos protocolos NFS (Network File System) e SAN (Storage Area Network) em um sistema de storage que esteja executando o ONTAP.
- Para sistemas Linux, os bancos de dados Oracle em VMDK e LUNs RDM são suportados quando você implementa o plug-in SnapCenter para VMware vSphere e Registra o plug-in com o SnapCenter.
- Suporta Mount Guard para AIX em sistemas de arquivos SAN e layout LVM.
- Suporta o Enhanced Journaled File System (JFS2) com Registro em linha em sistemas de arquivos SAN e layout LVM apenas para sistemas AIX.

  Dispositivos nativos SAN, sistemas de arquivos e layouts LVM criados em dispositivos SAN são suportados.

- Automatiza operações de backup, restauração e clone com reconhecimento de aplicações para sistemas de arquivos UNIX em seu ambiente SnapCenter

Plug-in do SnapCenter para recursos de banco de dados SAP HANA

Automatiza o backup, a restauração e a clonagem com reconhecimento de aplicações de bancos de dados SAP HANA em seu ambiente SnapCenter.

Recursos de plug-ins compatíveis com NetApp

Plug-ins compatíveis com NetApp são MongoDB, ORASCPM (aplicações Oracle), SAP ASE, SAP MaxDB e plug-in de storage.

- Oferece suporte a outros plug-ins para gerenciar aplicativos ou bancos de dados que não são compatíveis com outros plug-ins do SnapCenter. Os plug-ins compatíveis com NetApp não são fornecidos como parte da instalação do SnapCenter.
- Suporta a criação de cópias espelhadas de conjuntos de backup em outro volume e a execução de replicação de backup disco para disco.
- Suporta ambientes Windows e Linux.

Plug-in do SnapCenter para IBM DB2

Automatiza o backup, a restauração e a clonagem com reconhecimento de aplicações de bancos de dados IBM DB2 em seu ambiente SnapCenter.

Plug-in SnapCenter para PostgreSQL

Automatiza o backup, a restauração e a clonagem de instâncias do PostgreSQL com reconhecimento de aplicações no seu ambiente SnapCenter.

Plug-in SnapCenter para MySQL

Automatiza o backup, a restauração e a clonagem de instâncias do MySQL com reconhecimento de aplicações em seu ambiente SnapCenter.

Repositório SnapCenter

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

O banco de dados do repositório do servidor MySQL é instalado por padrão quando você instala o servidor SnapCenter. Se o servidor MySQL já estiver instalado e você estiver fazendo uma nova instalação do servidor SnapCenter, você deve desinstalar o servidor MySQL.

O SnapCenter suporta o MySQL Server 8.0.37 ou posterior como o banco de dados de repositório do SnapCenter. Se você estava usando uma versão anterior do servidor MySQL com uma versão anterior do SnapCenter, durante a atualização do SnapCenter, o servidor MySQL é atualizado para 8.0.37 ou posterior.

O repositório do SnapCenter armazena as seguintes informações e metadados:

- Metadados de backup, clone, restauração e verificação
- Informações sobre relatórios, trabalhos e eventos
- Informações de host e plug-in
- Detalhes de função, usuário e permissão
- Informações de conexão do sistema de armazenamento

Recursos de segurança

A SnapCenter emprega recursos rígidos 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 AES (Advanced Encryption Standard).
- O SnapCenter usa algoritmos de segurança compatíveis com o padrão Federal de processamento de informações (FIPS).
- O SnapCenter suporta o uso dos certificados de CA autorizados fornecidos pelo cliente.
- O SnapCenter 4.1.1 ou posterior suporta TLS (Transport Layer Security) 1,2 para comunicação com o ONTAP. Você também pode usar o TLS 1,2 para comunicação entre clientes e servidores.

  A partir de 5,0, o SnapCenter suporta TLS (TLS) 1,3 para comunicação com o ONTAP.

- O SnapCenter suporta um determinado conjunto de pacotes de criptografia SSL para fornecer segurança em toda a comunicação de rede.

  Para obter mais informações, "Como configurar o SSL Cipher Suite suportado"consulte .

- O SnapCenter é instalado no firewall da sua empresa para permitir o acesso ao servidor SnapCenter e para permitir a comunicação entre o servidor SnapCenter 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 é integrado ao Windows active Directory para login e controle de acesso baseado em função (RBAC) que regem as permissões de acesso.
- O IPsec é compatível com o SnapCenter no ONTAP para máquinas host Windows e Linux. "Saiba 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 desconetado em 5 minutos. Após 20 minutos de inatividade, o SnapCenter faz o logout e você deve fazer login novamente. Você pode modificar o período de logout.
- O início de sessão está temporariamente desativado após 5 ou mais tentativas de início de sessão incorretas.
- Suporta autenticação de certificado CA entre o servidor SnapCenter e o ONTAP. "Saiba mais".
- O verificador de integridade é adicionado ao servidor SnapCenter 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 servidor SnapCenter permite o suporte centralizado de certificados SSL durante a instalação. Para melhorar a comunicação segura entre o servidor e o plug-in, o SnapCenter suporta o uso dos certificados de CA autorizados fornecidos pelo cliente.

Você deve implantar certificados de CA depois de instalar o servidor SnapCenter e os respetivos plug-ins. Para obter mais informações, "Gerar arquivo CSR do certificado CA"consulte .

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

Comunicação SSL bidirecional

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

Visão geral da autenticação baseada em certificados

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

Autenticação multifator (MFA)

O MFA usa um provedor de identidade (IDP) de terceiros por meio da Security Assertion Markup Language (SAML) para gerenciar sessões de usuários. Esta funcionalidade melhora a segurança de autenticação, tendo a opção de utilizar vários fatores, como TOTP, biometria, notificações push, etc., juntamente com o nome de utilizador e palavra-passe 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 portfólio.

O MFA é aplicável apenas para login na IU do servidor SnapCenter. Os logins são autenticados por meio dos Serviços de Federação do ative Directory (AD FS) do IDP. 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 ativar o MFA no SnapCenter, você precisará dos metadados do AD FS.

Para obter informações sobre como ativar o MFA, "Ativar a autenticação multifator"consulte .

Controles de acesso baseados em função do SnapCenter (RBAC)

Tipos de RBAC

As permissões de controle de acesso baseado em função (RBAC) e ONTAP do SnapCenter permitem que os administradores do SnapCenter delegem o controle de recursos do SnapCenter a diferentes usuários ou grupos de usuários. Esse acesso gerenciado centralmente capacita os administradores de aplicativos a trabalhar com segurança em ambientes delegados.

Você pode criar e modificar funções e adicionar acesso a recursos aos usuários a qualquer momento, mas quando você estiver configurando o SnapCenter pela primeira vez, você deve pelo menos adicionar usuários ou grupo do ative Directory a 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 ative Directory do sistema operacional ou banco de dados.

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

- SnapCenter RBAC
- Plug-in RBAC do SnapCenter (para alguns plug-ins)
- RBAC no nível da aplicação

- Permissões da ONTAP

SnapCenter RBAC

Funções e permissões

O SnapCenter é fornecido com funções predefinidas com permissões já atribuídas. Você pode atribuir usuários ou grupos de usuários a essas funções. Você também pode criar novas funções e gerenciar permissões e usuários.

Atribuindo permissões a usuários ou grupos

Você pode atribuir permissões a usuários ou grupos para acessar objetos do SnapCenter, como hosts, conexões de storage e grupos de recursos. Não é possível alterar as permissões da função SnapCenterAdmin.

É possível atribuir permissões RBAC a usuários e grupos dentro da mesma floresta e a usuários pertencentes a diferentes florestas. Não é possível atribuir permissões RBAC a usuários pertencentes a grupos aninhados entre florestas.

> Se você criar uma função personalizada, ela deverá conter todas as permissões da função de administrador do SnapCenter. Se você copiar apenas algumas das permissões, por exemplo, Host add ou Host remove, não será possível executar essas operações.

Autenticação

Os usuários são obrigados a 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, depois de inserir credenciais de login, eles serão solicitados a especificar a função que desejam usar. Os usuários também são obrigados a fornecer autenticação para executar as APIs.

RBAC no nível da 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 Snapshot e proteção de dados em um ambiente SQL Server, você deve definir credenciais com as credenciais Windows ou SQL adequadas. O servidor SnapCenter autentica o conjunto de credenciais usando qualquer um dos métodos. Se você quiser executar operações de snapshot e proteção de dados em um ambiente de sistema de arquivos do Windows no storage ONTAP, a função de administrador do SnapCenter deve ter admin Privileges no host do Windows.

Da mesma forma, se você deseja executar operações de proteção de dados em um banco de dados Oracle e se a autenticação do sistema operacional (os) estiver desativada no host do banco de dados, você deve definir credenciais com o banco de dados Oracle ou as credenciais Oracle ASM. O servidor SnapCenter autentica as credenciais definidas usando um desses métodos, dependendo da operação.

Plug-in do SnapCenter para 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 é compatível com o vCenter Server RBAC e o Data ONTAP RBAC.

Para obter informações, consulte "Plug-in do SnapCenter para VMware vSphere RBAC"

Permissões da ONTAP

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

Para obter informações sobre como criar a conta e atribuir permissões, consulte "Crie uma função de cluster do ONTAP com Privileges mínimo"

Permissões e funções do RBAC

O controle de acesso baseado em função (RBAC) do SnapCenter permite criar funções e atribuir permissões a essas funções e, em seguida, atribuir usuários ou grupos de usuários às funções. Isso permite que os administradores do SnapCenter criem um ambiente gerenciado centralmente, enquanto os administradores de aplicativos podem gerenciar tarefas de proteção de dados. O SnapCenter é fornecido com algumas funções e permissões predefinidas.

Funções do SnapCenter

O SnapCenter é fornecido com as seguintes funções predefinidas. Você pode atribuir usuários e grupos a essas funções ou criar novas funções.

Quando você atribui uma função a um usuário, somente os trabalhos relevantes a esse usuário são visíveis na página trabalhos, a menos que você tenha atribuído a função Administrador do SnapCenter.

- App Backup e Clone Admin
- Visualizador de cópias de segurança e clones
- Administrador de infraestrutura
- SnapCenterAdmin

Plug-in do SnapCenter para funções do VMware vSphere

Para gerenciar a proteção de dados consistente com VM de VMs, VMDKs e armazenamentos de dados, as funções a seguir são criadas no vCenter pelo plug-in do SnapCenter para VMware vSphere:

- Administrador do SCV
- Vista SCV
- Backup da VCR
- Restauração da VCR
- Restauração do arquivo convidado SCV

Para obter mais informações, consulte "Tipos de plug-in RBAC para SnapCenter para usuários do VMware vSphere"

Prática recomendada: a NetApp recomenda que você crie uma função do ONTAP para o plug-in do SnapCenter para operações do VMware vSphere e atribua a ele todos os Privileges necessários.

Permissões do SnapCenter

O SnapCenter fornece as seguintes permissões:

- Grupo recursos
- Política
- Backup
- Host
- Ligação de armazenamento
- Clone
- Provisionamento (apenas para banco de dados Microsoft SQL)
- Painel de instrumentos
- Relatórios
- Restaurar
- Recurso

  Os plug-in Privileges são necessários do administrador para que não administradores realizem operações de descoberta de recursos.

- Instalação ou desinstalação do plug-in

  Quando você ativa permissões de instalação de plug-in, você também deve modificar a permissão de host para habilitar leituras e atualizações.

- Migração
- Montar (apenas para banco de dados Oracle)
- Desmontar (apenas para banco de dados Oracle)
- Monitor de trabalho

  A permissão Monitor de tarefas permite que membros de diferentes funções vejam as operações em todos os objetos aos quais são atribuídos.

Funções e permissões do SnapCenter predefinidas

O SnapCenter é fornecido com funções predefinidas, cada uma com um conjunto de permissões já ativadas. Ao configurar e administrar o controle de acesso baseado em funções (RBAC), você pode usar essas funções predefinidas ou criar novas.

O SnapCenter inclui as seguintes funções predefinidas:

- Função de administrador do SnapCenter
- Função de Administrador de cópia de Segurança e Clonagem de aplicações
- Função Visualizador de cópia de Segurança e Clonagem
- Função de administrador de infraestrutura

Ao adicionar um usuário a uma função, você deve atribuir a permissão StorageConnection para habilitar a

comunicação de máquina virtual de armazenamento (SVM) ou atribuir um SVM ao usuário para habilitar a permissão para usar o SVM. A permissão Storage Connection permite que os usuários criem conexões SVM.

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

Função de administrador do SnapCenter

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

Função de Administrador de cópia de Segurança e Clonagem de aplicações

A função App Backup and Clone Admin tem as permissões necessárias para executar ações administrativas para backups de aplicativos e tarefas relacionadas a clones. Essa função não tem permissões para gerenciamento de host, provisionamento, gerenciamento de conexão de storage ou instalação remota.

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Grupo recursos	Não aplicável	Sim	Sim	Sim	Sim
Política	Não aplicável	Sim	Sim	Sim	Sim
Backup	Não aplicável	Sim	Sim	Sim	Sim
Host	Não aplicável	Sim	Sim	Sim	Sim
Ligação de armazenamento	Não aplicável	Não	Sim	Não	Não
Clone	Não aplicável	Sim	Sim	Sim	Sim
Provisionamento	Não aplicável	Não	Sim	Não	Não
Painel de instrumentos	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 do plug-in	Não	Não aplicável		Não aplicável	Não aplicável

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Montagem	Sim	Sim	Não aplicável	Não aplicável	Não aplicável
Desmontar	Sim	Sim	Não aplicável	Não aplicável	Não aplicável
Restauração completa do volume	Não	Não	Não aplicável	Não aplicável	Não aplicável
Monitor de trabalho	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Função Visualizador de cópia de Segurança e Clonagem

A função Visualizador de cópia de Segurança e Clonagem tem uma vista só de leitura de todas as permissões. Essa função também tem permissões habilitadas para descoberta, geração de relatórios e acesso ao Dashboard.

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Grupo recursos	Não aplicável	Não	Sim	Não	Não
Política	Não aplicável	Não	Sim	Não	Não
Backup	Não aplicável	Não	Sim	Não	Não
Host	Não aplicável	Não	Sim	Não	Não
Ligação de armazenamento	Não aplicável	Não	Sim	Não	Não
Clone	Não aplicável	Não	Sim	Não	Não
Provisionamento	Não aplicável	Não	Sim	Não	Não
Painel de instrumentos	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

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Instalação/desinstalação do plug-in	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Montagem	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Desmontar	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restauração completa do volume	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Monitor de trabalho	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 storage, provisionamento, grupos de recursos, relatórios de instalação remota e acesso ao Dashboard.

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Grupo recursos	Não aplicável	Sim	Sim	Sim	Sim
Política	Não aplicável	Não	Sim	Sim	Sim
Backup	Não aplicável	Sim	Sim	Sim	Sim
Host	Não aplicável	Sim	Sim	Sim	Sim
Ligação de armazenamento	Não aplicável	Sim	Sim	Sim	Sim
Clone	Não aplicável	Não	Sim	Não	Não
Provisionamento	Não aplicável	Sim	Sim	Sim	Sim
Painel de instrumentos	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Relatórios	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Permissões	Ativado	Criar	Leia	Atualização	Eliminar
Restaurar	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Recurso	Sim	Sim	Sim	Sim	Sim
Instalação/desinstalação do plug-in	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Migração	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Montagem	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Desmontar	Não	Não aplicável	Não aplicável	Não aplicável	Não aplicável
Restauração completa do volume	Não	Não	Não aplicável	Não aplicável	Não aplicável
Monitor de trabalho	Sim	Não aplicável	Não aplicável	Não aplicável	Não aplicável

Recuperação de desastres do SnapCenter

Você pode recuperar o servidor SnapCenter em caso de desastres como corrupção de recursos ou falha do servidor usando o recurso recuperação de desastres (DR) do SnapCenter. Você pode recuperar o repositório do SnapCenter, as programações do servidor e os componentes de configuração do servidor. Você também pode recuperar o plug-in do SnapCenter para SQL Server e o plug-in do SnapCenter para armazenamento de dados SQL Server.

Esta seção descreve os dois tipos de recuperação de desastres (DR) no SnapCenter:

DR do servidor SnapCenter

- Os dados do servidor SnapCenter são copiados e podem ser recuperados sem nenhum plug-in adicionado ou gerenciado pelo servidor SnapCenter.
- O servidor SnapCenter secundário deve ser instalado no mesmo diretório de instalação e na mesma porta que o servidor SnapCenter primário.
- Para autenticação multifator (MFA), durante o DR do servidor SnapCenter, feche todas as guias do navegador e reabra um navegador para fazer login novamente. Isso apagará 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 servidor SnapCenter. "Workflows de API REST para recuperação de desastres do servidor SnapCenter"Consulte .
- 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. Deve repetir manualmente as definições do

registo de auditoria.

Plug-in do SnapCenter e recuperação de desastres de storage

O DR é compatível apenas com o plug-in SnapCenter para SQL Server. Quando o plug-in do SnapCenter estiver inativo, mude para um host SQL diferente e recupere os dados executando algumas etapas. "Recuperação de desastres do plug-in SnapCenter para SQL Server"Consulte .

A SnapCenter usa a tecnologia ONTAP SnapMirror para replicar dados. Ele pode ser usado para replicar dados para um local secundário para recuperação de desastres e mantê-los sincronizados. Um failover pode ser iniciado quebrando a relação de replicação no SnapMirror. Durante o failback, a sincronização pode ser revertida e os dados do local de DR podem ser replicados de volta para o local principal.

Recursos, grupos de recursos e políticas

Antes de usar o SnapCenter, é útil entender 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** são normalmente bancos de dados, sistemas de arquivos do Windows ou compartilhamentos de arquivos que você faz backup ou clone com o SnapCenter.

  No entanto, dependendo do seu ambiente, os recursos podem ser instâncias de banco de dados, grupos de disponibilidade do Microsoft SQL Server, bancos de dados Oracle RAC, sistemas de arquivos do Windows ou um grupo de aplicativos personalizados.

- Um **grupo de recursos** é uma coleção de recursos em um host ou cluster. O grupo de recursos também pode conter recursos de vários hosts e vários clusters.

  Quando você executa uma operação em um grupo de recursos, executa essa operação em todos os recursos definidos no grupo de recursos de acordo com a programação especificada para o grupo de recursos.

  Você pode fazer backup sob demanda de um único recurso ou de um grupo de recursos. Você também pode configurar backups programados para recursos únicos e grupos de recursos.

  > Se você colocar um host de um grupo de recursos compartilhados no modo de manutenção e se houver programações associadas ao mesmo grupo de recursos compartilhados, todas as operações agendadas serão suspensas para todos os outros hosts do grupo de recursos compartilhados.

  Você deve usar um plug-in de banco de dados para fazer backup de bancos de dados, um plug-in de sistema de arquivos para fazer backup de sistemas de arquivos e o plug-in SnapCenter para VMware vSphere para fazer backup de VMs e datastores.

- **Políticas** especificam a frequência de backup, retenção de cópia, replicação, scripts e outras caraterísticas das operações de proteção de dados.

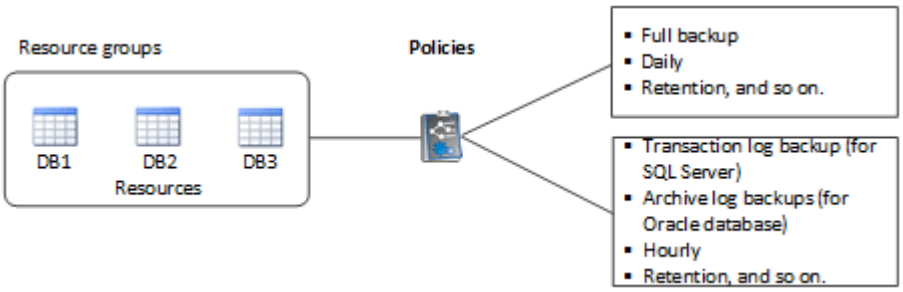
  Ao criar um grupo de recursos, você seleciona uma ou mais políticas para esse grupo. Você também pode selecionar uma política ao executar um backup sob demanda.

Pense em um grupo de recursos como definindo *o que* você quer proteger e quando você quer protegê-lo em termos de dia e tempo. Pense em uma política como definindo *como* você quer protegê-la. Se você estiver fazendo backup de todos os bancos de dados ou fazendo backup de todos os sistemas de arquivos de um

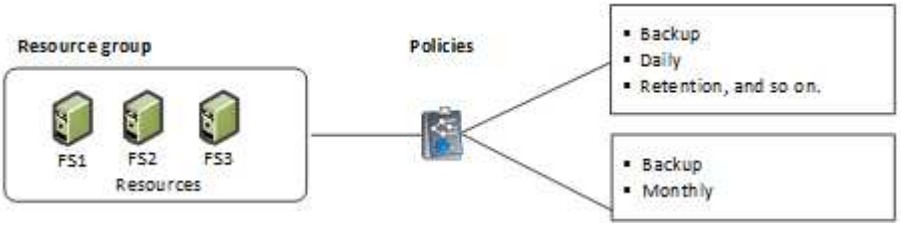
host, por exemplo, você pode criar um grupo de recursos que inclua todos os bancos de dados ou todos os sistemas de arquivos no host. Em seguida, você pode anexar duas políticas ao grupo de recursos: Uma política diária e uma política por hora.

Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diário e outro agendamento que executa backups de log por hora.

A imagem a seguir ilustra a relação entre recursos, grupos de recursos e políticas para bancos de dados:



A imagem a seguir ilustra a relação entre recursos, grupos de recursos e políticas para sistemas de arquivos do Windows:



Prescripts e postscripts

Você pode usar prescripts e postscripts personalizados como parte de suas operações de proteção de dados. Esses scripts habilitam a automação antes do trabalho de proteção de dados ou depois. Por exemplo, você pode incluir um script que o notifica automaticamente sobre falhas ou avisos de trabalhos de proteção de dados. Antes de configurar suas prescriptas e pós-scripts, você deve entender alguns dos requisitos para criar esses scripts.

Tipos de script suportados

Os seguintes tipos de scripts são suportados para o Windows:

- Arquivos em lote
- Scripts do PowerShell
- Scripts Perl

Os seguintes tipos de scripts são suportados para UNIX:

- Scripts Perl
- Scripts Python
- Scripts de shell

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

Caminho do script

Todos os prescripts e pós-scripts executados como parte das operações do SnapCenter, em sistemas de storage não virtualizados e virtualizados, são executados no host do plug-in.

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

O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_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 nas políticas de backup. Quando um trabalho de backup é iniciado, a diretiva associa automaticamente o script aos recursos que estão sendo copiados. Ao criar uma política de backup, você pode especificar os argumentos prescritor e postscript.

Não é possível especificar vários scripts.

Tempos limite de script

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

Saída de script

O diretório padrão para os arquivos de saída de prescripts e postscripts do Windows é o Windows System32.

Não há local padrão para as prescripts e postscripts UNIX. Você pode redirecionar o arquivo de saída para qualquer local preferido.

Automação da SnapCenter usando APIS REST

Você pode usar APIS REST para executar várias 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 para exibir a documentação da API REST, bem como emitir manualmente uma chamada de API. Você pode usar APIS REST para ajudar a gerenciar seu servidor SnapCenter ou seu host do SnapCenter vSphere.

As APIs REST para…	Este hotel fica bem perto…
Servidor SnapCenter	Https:// cliente SnapCenter_IP_address_or_name>: Cliente SnapCenter_port>/swagger/

As APIs REST para…	Este hotel fica bem perto…
Plug-in do SnapCenter para VMware vSphere	/<OVA_IP_address_or_host_name>:<scv_plugin_port>/api/swagger-ui.html

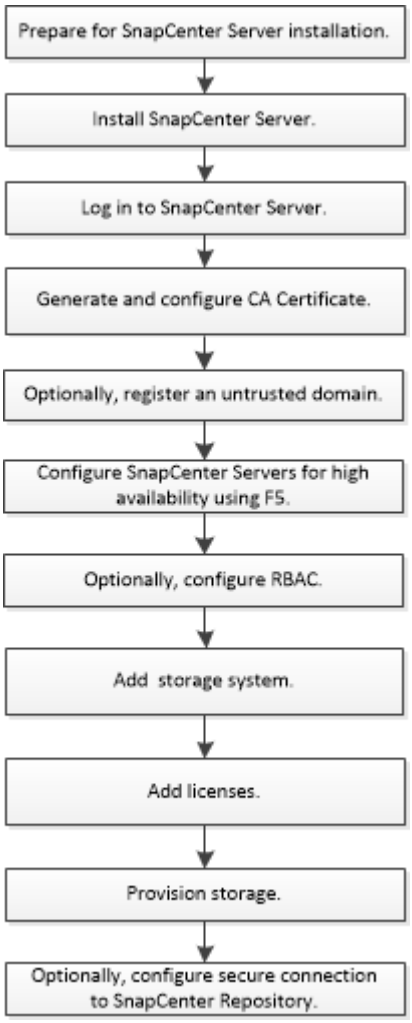
Para obter informações sobre APIS REST do SnapCenter, consulte "Visão geral das APIs REST"

Para obter informações sobre o plug-in do SnapCenter para APIs REST do VMware vSphere, consulte "Plug-in do SnapCenter para APIs REST do VMware vSphere"

Instalação do servidor SnapCenter

Fluxo de trabalho de instalação

O fluxo de trabalho mostra as diferentes tarefas necessárias para instalar e configurar o servidor SnapCenter.



Prepare-se para instalar o servidor SnapCenter

Requisitos de domínio e grupo de trabalho

O servidor SnapCenter pode ser instalado em sistemas que estejam em um domínio ou em um grupo de trabalho. O usuário usado para instalação deve ter Privileges de administrador na máquina no caso de grupo de trabalho e domínio.

Para instalar plug-ins do servidor SnapCenter e do SnapCenter em hosts Windows, você deve usar um dos seguintes:

- **Domínio ative 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 do Windows.

- **Grupos de trabalho**

  Você deve usar uma conta local que tenha direitos de administrador local.

Embora as trusts de domínio, florestas de vários domínios e trusts de vários domínios sejam suportados, os domínios de floresta cruzada não são suportados. A documentação da Microsoft sobre domínios e trusts do ative Directory contém mais informações.

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

Requisitos de espaço e dimensionamento

Antes de instalar o servidor SnapCenter, você deve estar familiarizado com os requisitos de espaço e dimensionamento. Você também deve aplicar as atualizações de sistema e segurança disponíveis.

Item	Requisitos de host do Windows	Requisitos de host do Linux
Sistemas operacionais	Microsoft Windows Apenas as versões em inglês, alemão, japonês e chinês simplificado dos sistemas operacionais são suportadas. Para obter as informações mais recentes sobre versões suportadas, "Ferramenta de Matriz de interoperabilidade do NetApp"consulte .	• Red Hat Enterprise Linux (RHEL) 8 e 9 • SUSE Linux Enterprise Server (SLES) 15 Para obter as informações mais recentes sobre versões suportadas, "Ferramenta de Matriz de interoperabilidade do NetApp"consulte .
Contagem mínima de CPU	4 núcleos	4 núcleos
RAM mínima	8 GB O pool de buffers do MySQL Server usa 20% do total de RAM.	8 GB

Item	Requisitos de host do Windows	Requisitos de host do Linux
Espaço mínimo no disco rígido para o software e logs do servidor SnapCenter	7 GB Se você tiver o repositório SnapCenter na mesma unidade em que o servidor SnapCenter está instalado, então é recomendável ter 15 GB.	15 GB
Espaço mínimo no disco rígido para o repositório SnapCenter	8 GB OBSERVAÇÃO: Se você tiver o servidor SnapCenter na mesma unidade em que o repositório SnapCenter está instalado, então é recomendável ter 15 GB.	Não aplicável
Pacotes de software necessários	• Microsoft .NET Framework 4.7.2 ou posterior • Pacote de Hospedagem ASP.NET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell 7.4.2 ou posterior Para obter informações específicas de solução de problemas .NET, "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet" consulte .	• ASP.NET Core Runtime começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell 7.4.2 ou posterior • O nginx é um servidor web que pode ser usado como proxy reverso • PAM-devel PAM (Pluggable Authentication Modules) é uma ferramenta de segurança do sistema que permite que os administradores de sistema definam a política de autenticação sem ter que recompilar programas que fazem a autenticação.

Requisitos de host SAN

Se o seu host SnapCenter fizer parte de um ambiente FC/iSCSI, talvez seja necessário instalar software adicional no sistema para permitir o acesso ao storage ONTAP.

O SnapCenter não inclui Utilitários do anfitrião ou um DSM. Se o seu host SnapCenter fizer parte de um ambiente SAN, talvez seja necessário instalar e configurar o seguinte software:

- Utilitários do host

  Os Utilitários de host são compatíveis com FC e iSCSI e permitem que você use o MPIO em seus servidores Windows. Para obter informações, "Documentação dos utilitários do host"consulte .

- Microsoft DSM para Windows MPIO

  Este software funciona com drivers MPIO do Windows para gerenciar vários caminhos entre computadores host NetApp e Windows.

  É necessário um DSM para configurações de alta disponibilidade.

  > ⓘ Se estiver a utilizar o ONTAP DSM, deve migrar para o Microsoft DSM. Para obter mais informações, "Como migrar do ONTAP DSM para o Microsoft DSM"consulte .

Sistemas e aplicações de storage compatíveis

Você deve conhecer o sistema de storage compatível, as aplicações e os bancos de dados.

- O SnapCenter oferece suporte ao ONTAP 9.12.1 e posterior para proteger seus dados.
- O SnapCenter oferece suporte ao Amazon FSX for NetApp ONTAP para proteger seus dados da versão de patch do software SnapCenter 4,5 P1.

  Se você estiver usando o Amazon FSX for NetApp ONTAP, verifique se os plug-ins de host do servidor SnapCenter são atualizados para 4,5 P1 ou posterior para executar operações de proteção de dados.

  É compatível com NVMe (non-volátil Memory Express) em Transport Control Protocol (TCP).

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

- 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, "Ferramenta de Matriz de interoperabilidade do NetApp" consulte .

- O SnapCenter 4,9 P1 e posterior oferece suporte à proteção de workloads Oracle e Microsoft SQL em ambientes de data center definido por software (SDDC) da Amazon Web Services (AWS).

  Para obter mais informações, "Proteja workloads Oracle e MS SQL usando o NetApp SnapCenter em ambientes AWS SDDC"consulte .

Navegadores suportados

O software SnapCenter pode ser usado em vários navegadores.

- Chrome versão 125 e posterior

- Microsoft Edge 110.0.1587.17 e posterior

Para obter as informações mais recentes sobre versões suportadas, consulte : "Ferramenta de Matriz de interoperabilidade do NetApp".

Requisitos de conexão e porta

Você deve garantir que os requisitos de conexões e portas sejam atendidos antes de instalar os plug-ins do servidor SnapCenter e do aplicativo ou do banco de dados.

- Os aplicativos não podem compartilhar uma porta.

  Cada porta deve ser dedicada ao aplicativo apropriado.

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

  Você pode alterar uma porta de plug-in após a instalação usando o assistente Modificar host.

- 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, adicione uma regra de firewall no host do plug-in para essa porta para o Loader de plug-ins do SnapCenter.

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

Tipo de porta	Porta predefinida
Porta da web do SnapCenter	8146 (HTTPS), bidirecional, personalizável, como no URL *https://server:8146* Usado para comunicação entre o cliente SnapCenter (o usuário SnapCenter) e o servidor SnapCenter. Também usado para comunicação dos hosts de plug-in para o servidor SnapCenter. Para personalizar a porta, consulte "Instale o servidor SnapCenter usando o assistente de instalação."
Porta de comunicação SnapCenter SMCore	8145 (HTTPS), bidirecional, personalizável A porta é usada para comunicação entre o servidor SnapCenter e os hosts onde os plug-ins do SnapCenter estão instalados. Para personalizar a porta, consulte "Instale o servidor SnapCenter usando o assistente de instalação."

Tipo de porta	Porta predefinida
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 dentro do host do servidor SnapCenter de maneira centralizada. Para personalizar a porta, consulte "Instale o servidor SnapCenter usando o assistente de instalação."
Porto RabbitMQ	5672 (tcp) Esta é a porta padrão em que o RabbitMQ escuta e é usada para comunicação entre o serviço de Agendador e o SnapCenter.
Porta MySQL	3306 (HTTPS), bidirecional, personalizável A porta é usada para comunicação entre o SnapCenter e o banco de dados do repositório MySQL. Você pode criar conexões seguras do servidor SnapCenter para o servidor MySQL. "Saiba mais" Para personalizar a porta, consulte "Instale o servidor SnapCenter usando o assistente de instalação."
Hosts de plug-in do Windows	135, 445 (TCP) Além das portas 135 e 445, o intervalo de portas dinâmico especificado pela Microsoft também deve estar aberto. As operações de instalação remota usam o serviço Windows Management Instrumentation (WMI), que procura dinamicamente esse intervalo de portas. Para obter informações sobre o intervalo de portas dinâmico suportado, consulte "Visão geral do serviço e requisitos de porta de rede para Windows" As portas são usadas para comunicação entre o servidor SnapCenter e o host no qual o plug-in está sendo instalado. Para enviar binários de pacotes de plug-in para hosts de plug-in do Windows, as portas devem estar abertas apenas no host de plug-in e podem ser fechadas após a instalação.

Tipo de porta	Porta predefinida
Hosts plug-in Linux ou AIX	22 (SSH) As portas são usadas para comunicação entre o servidor SnapCenter e o host onde o plug-in está sendo instalado. As portas são usadas pelo SnapCenter para copiar binários de pacotes de plug-in para hosts de plug-in Linux ou AIX e devem ser abertas ou excluídas do firewall ou iptables.
Pacote de plug-ins do SnapCenter para Windows, pacote de plug-ins do SnapCenter para Linux ou pacote de plug-ins do SnapCenter para AIX	8145 (HTTPS), bidirecional, personalizável A porta é usada para comunicação entre SMCore e hosts onde o pacote plug-ins está instalado. O caminho de comunicação também precisa ser aberto entre o LIF de gerenciamento da SVM e o servidor SnapCenter. Para personalizar a porta, consulte "Adicione hosts e instale o plug-in do SnapCenter para Microsoft Windows" ou "Adicione hosts e instale o pacote de plug-ins do SnapCenter para Linux ou AIX."
Plug-in SnapCenter para banco de dados Oracle	27216, personalizável A porta JDBC padrão é usada pelo plug-in para Oracle para conexão com o banco de dados Oracle. Para personalizar a porta, consulte "Adicione hosts e instale o pacote de plug-ins do SnapCenter para Linux ou AIX."
Plug-in do SnapCenter para banco de dados do Exchange	909, personalizável A porta NET.TCP padrão é usada pelo plug-in para Windows para conetar-se aos retornos de chamada do Exchange VSS. Para personalizar a porta, "Adicione hosts e instale o Plug-in para o Exchange"consulte .
Plug-ins compatíveis com NetApp para SnapCenter	9090 (HTTPS), fixo Esta é uma porta interna usada somente no host de plug-in suportado pela NetApp; nenhuma exceção de firewall é necessária. A comunicação entre o SnapCenter Server e os plug-ins suportados pelo NetApp é roteada pela porta 8145.

Tipo de porta	Porta predefinida
Porta de comunicação do cluster ONTAP ou SVM	443 (HTTPS), bidirectional80 (HTTP), bidirecional A porta é usada pela sal (camada de abstração de storage) para comunicação entre o host que executa o servidor SnapCenter e o SVM. Atualmente, a porta também é usada pelo sal em hosts plug-in do SnapCenter para Windows para comunicação entre o host do plug-in do SnapCenter e o SVM.
Plug-in do SnapCenter para o banco de dados SAP HANA vCode Spell Checkerports	3instance_number13 ou 3instance_number15, HTTP ou HTTPS, bidirecional e personalizável Para um locatário único de contentor de banco de dados multitenant (MDC), o número da porta termina com 13; para não MDC, o número da porta termina com 15. Por exemplo, 32013 é o número da porta, por exemplo, 20 e 31015 é o número da porta, por exemplo, 10. Para personalizar a porta, consulte "Adicione hosts e instale pacotes plug-in em hosts remotos."
Porta de comunicação do controlador de domínio	Consulte a documentação da Microsoft para identificar as portas que devem ser abertas no firewall em um controlador de domínio para que a autenticação funcione corretamente. É necessário abrir as portas necessárias da Microsoft no controlador de domínio para que o servidor SnapCenter, os hosts Plug-in ou outro cliente Windows possam autenticar os usuários.

Para modificar os detalhes da porta, "Modificar hosts de plug-in"consulte .

Licenças 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 licenças do SnapCenter que você instala depende do ambiente de storage e dos recursos que deseja usar.

Licença	Quando necessário
Baseado em controladora padrão da SnapCenter	Necessário para FAS, AFF e All SAN Array (ASA) A licença padrão da SnapCenter é uma licença baseada em controlador e está incluída como parte do ONTAP One. Se você tiver a licença do SnapManager Suite, você também obtém o direito de licença padrão do SnapCenter. Se você quiser instalar o SnapCenter em uma base de avaliação com o storage FAS, AFF ou ASA, poderá obter uma licença de avaliação do ONTAP One entrando em Contato com o representante de vendas. Para obter informações sobre as licenças incluídas no ONTAP One, "Licenças incluídas no ONTAP One" consulte . O SnapCenter também é oferecido como parte do pacote de proteção de dados. Se você comprou o A400 ou posterior, você deve comprar o pacote de proteção de dados.
SnapMirror ou SnapVault	ONTAP A licença SnapMirror ou SnapVault é necessária se a replicação estiver ativada no SnapCenter.
SnapRestore	Necessário para restaurar e verificar backups. Em sistemas de storage primário • Necessário nos sistemas de destino do SnapVault para executar a verificação remota e restaurar a partir de um backup. • Necessário nos sistemas de destino SnapMirror para efetuar a verificação remota.
FlexClone	Necessário clonar bancos de dados e operações de verificação. Em sistemas de storage primário e secundário • Necessário nos sistemas de destino do SnapVault para criar clones a partir do backup do Vault secundário. • Necessário nos sistemas de destino do SnapMirror para criar clones do backup secundário do SnapMirror.

Licença	Quando necessário
Protocolos	• Licença iSCSI ou FC para LUNs • Licença CIFS para compartilhamentos SMB • Licença NFS para VMDKs do tipo NFS • Licença iSCSI ou FC para VMDKs do tipo VMFS Necessário nos sistemas de destino do SnapMirror para fornecer dados se um volume de origem não estiver disponível.
Licenças padrão da SnapCenter (opcional)	Destinos secundários É recomendado, mas não obrigatório, que você adicione licenças padrão do SnapCenter a destinos secundários. Se as licenças padrão do SnapCenter 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, é necessária uma licença FlexClone em destinos secundários para executar operações de clonagem e verificação.

As licenças do SnapCenter Advanced e do 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 o 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, "Adicione licenças padrão baseadas em controladora SnapCenter"consulte .

Licenças SMBR (Single Mailbox Recovery)

Se você estiver usando o plug-in do SnapCenter para gerenciar bancos de dados do Microsoft Exchange Server e a recuperação de caixa de correio única (SMBR), você precisará de licença adicional para SMBR, que precisa ser adquirida separadamente com base na caixa de correio do usuário.

A recuperação de caixa de correio única NetApp chegou ao fim da disponibilidade (EOA) em 12 de maio de 2023. Para obter mais informações, "CPC-00507"consulte . A NetApp continuará a oferecer suporte a clientes que adquiriram capacidade, manutenção e suporte da caixa de correio por meio de números de peça de marketing introduzidos em 24 de junho de 2020, durante o período do direito ao suporte.

O NetApp Single Mailbox Recovery é um produto parceiro fornecido pela Ontrack. O Ontrack PowerControls oferece recursos semelhantes aos da recuperação de caixa de correio única do NetApp. Os clientes podem adquirir novas licenças de software Ontrack PowerControls e renovações de manutenção e suporte Ontrack PowerControls do Ontrack (até licensingteam@ontrack.com) para recuperação granular da caixa de correio após a data EOA de 12 de maio de 2023.

Registe-se para aceder ao software SnapCenter

Você pode acessar o software SnapCenter se você é novo no Amazon FSX for NetApp ONTAP ou Azure NetApp Files e não tem uma conta NetApp existente.

Antes de começar

- Você deve ter acesso ao ID de e-mail corporativo.
- Se você usa o Azure NetApp Files, você deve ter o ID de assinatura do Azure.
- Se você estiver usando o Amazon FSX for NetApp ONTAP, você deve ter o ID do sistema de arquivos do seu sistema de arquivos FSX for 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 site de suporte da NetApp (NSS) para acesso "completo" a partir do acesso "convidado".

Passos

1. Clique https://mysupport.netapp.com/site/user/registration para inscrição.
2. Insira seu ID de e-mail corporativo, preencha o captcha e aceite a política de privacidade do NetApp e clique em **Enviar**.
3. Autentique o Registro inserindo a OTP enviada para seu ID de e-mail e clique em **continuar**.
4. Na página de conclusão do registo, introduza os seguintes detalhes para concluir o registo.
   a. Selecione **Cliente NetApp / Usuário final**.
   b. No campo DE NÚMERO DE SÉRIE, insira um dos seguintes itens:
      - ID de subscrição do Azure se estiver a utilizar o Azure NetApp Files.
      - ID do sistema de arquivos se você estiver usando o Amazon FSX for NetApp ONTAP.

Você pode levantar um ticket em https://mysupport.netapp.com/site/help se você enfrentar qualquer problema durante o Registro ou para saber o status.

Métodos de autenticação para suas credenciais

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

Autenticação do Windows

O método de autenticação do Windows é autenticado no ative Directory. Para autenticação do Windows, o ative Directory é configurado fora do SnapCenter. O SnapCenter se autentica sem configuração adicional. Você precisa de uma credencial do Windows para executar tarefas como adicionar hosts, instalar pacotes de plug-in e agendar tarefas.

Autenticação de domínio não confiável

O SnapCenter permite a criação de credenciais do Windows usando usuários e grupos pertencentes aos domínios não confiáveis. Para que a autenticação seja bem-sucedida, você deve Registrar os domínios não

confiáveis com o SnapCenter.

Autenticação local do grupo de trabalho

O SnapCenter permite a criação de credenciais do Windows com usuários e grupos de trabalho locais. A autenticação do Windows para usuários e grupos de grupos de trabalho locais não acontece no momento da criação de credenciais do Windows, mas é adiada até que o Registro do host e outras operações de host sejam executadas.

Autenticação do SQL Server

O método de autenticação SQL é autenticado 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 recursos. Você precisa de autenticação do SQL Server para executar operações como agendamento no SQL Server ou descoberta de recursos.

Autenticação Linux

O método de autenticação Linux é autenticado em um host Linux. Você precisa de autenticação Linux durante a etapa inicial de adicionar o host Linux e instalar o pacote de plug-ins do SnapCenter remotamente a partir da GUI do SnapCenter.

Autenticação AIX

O método de autenticação AIX é autenticado em um host AIX. Você precisa de autenticação AIX durante a etapa inicial de adicionar o host AIX e instalar o pacote de plug-ins do SnapCenter para AIX remotamente a partir da GUI do SnapCenter.

Autenticação de banco de dados Oracle

O método de autenticação de banco de dados Oracle é autenticado 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 (os) estiver desativada 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 sysdba Privileges.

Autenticação Oracle ASM

O método de autenticação Oracle ASM é autenticado em uma instância do Oracle Automatic Storage Management (ASM). Se for necessário acessar a instância do Oracle ASM e se a autenticação do sistema operacional (os) estiver desativada no host do banco de dados, você precisará de uma autenticação Oracle ASM. Portanto, antes de adicionar uma credencial Oracle ASM, você deve criar um usuário Oracle com sysasm Privileges na instância ASM.

Autenticação de catálogo RMAN

O método de autenticação de catálogo RMAN é autenticado no banco de dados de catálogo do Oracle Recovery Manager (RMAN). Se você configurou um mecanismo de catálogo externo e registrou seu banco de dados no banco de dados de catálogo, você precisa adicionar autenticação de catálogo RMAN.

Conexões e credenciais de storage

Antes de executar operações de proteção de dados, você deve configurar as conexões

de armazenamento e adicionar as credenciais que o servidor SnapCenter e os plug-ins SnapCenter usarão.

- * Conexões de armazenamento*

  As conexões de armazenamento dão aos plug-ins do servidor SnapCenter e do SnapCenter acesso ao armazenamento do ONTAP. A configuração dessas conexões também envolve a configuração de 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 no qual você está instalando o plug-in do SnapCenter. Formatos válidos para o campo Nome de usuário são:

    - *NetBIOS_username*
    - *Domain FQDN_username*
    - *upn*
  - Administrador local (apenas para grupos de trabalho)

    Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host.

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

  - Credenciais para grupos de recursos individuais

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

Autenticação multifator (MFA)

Gerenciamento da autenticação multifator (MFA)

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

Habilitar a autenticação multifator (MFA)

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

Sobre esta tarefa

- O SnapCenter suporta logins baseados em SSO quando outros aplicativos são configurados no mesmo AD FS. Em certas configurações do AD FS, o SnapCenter pode exigir autenticação de 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`o . Alternativamente, você também pode "Guia de

referência de cmdlet do software SnapCenter"ver .

Antes de começar

- O Serviço de Federação do ative Directory do Windows (AD FS) deve estar ativo e em execução no respetivo domínio.
- Você deve ter um serviço de autenticação multifator compatível com AD FS, como Azure MFA, Cisco Duo, etc.
- O carimbo de data/hora do servidor SnapCenter e AD FS deve ser o mesmo, independentemente do fuso horário.
- Procure e configure o certificado de CA autorizado para o servidor SnapCenter.

  O certificado CA é obrigatório pelos seguintes motivos:

  - Garante que as comunicações ADFS-F5 não quebrem porque os certificados autoassinados são exclusivos no nível do nó.
  - Garante que durante a atualização, reparo ou 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, "Gerar arquivo CSR do certificado CA"consulte .

Passos

1. Conete-se ao host dos Serviços de Federação do ative Directory (AD FS).
2. Faça download do arquivo de metadados de federação do AD FS de "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copie o arquivo baixado para o servidor SnapCenter para ativar o recurso MFA.
4. Faça login no servidor SnapCenter como o usuário Administrador do SnapCenter através 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 servidor SnapCenter.
6. Copie o arquivo gerado para o host do AD FS para configurar o SnapCenter como a entidade cliente.
7. Habilite o MFA para servidor SnapCenter usando `Set-SmMultiFactorAuthentication` o cmdlet.
8. (Opcional) Verifique o status e as configurações do MFA usando `Get-SmMultiFactorAuthentication` o cmdlet.
9. Vá para o console de gerenciamento da Microsoft (MMC) e execute as seguintes etapas:
   a. Clique em **File** > **Add/Remove Snapin**.
   b. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
   c. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
   d. Clique em **raiz da consola** > **certificados – computador local** > **Pessoal** > **certificados**.
   e. Clique com o botão direito do rato no certificado CA vinculado ao SnapCenter e selecione **todas as tarefas** > **gerir chaves privadas**.

f. No assistente de permissões, execute as seguintes etapas:

i. Clique em **Add**.

ii. Clique em **locais** e selecione o host em questão (topo da hierarquia).

iii. Clique em **OK** na janela pop-up **Locations**.

iv. No campo Nome do objeto, digite 'IIS_IUSRS' e 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 do rato em **confiar em parte** > **Adicionar confiança de parte dependente** > **Iniciar**.
    b. Selecione a segunda opção e navegue no arquivo de metadados do SnapCenter MFA e clique em **Avançar**.
    c. Especifique um nome de exibição e clique em **Next**.
    d. Escolha uma política de controle de acesso conforme necessário e clique em **Next**.
    e. Selecione as configurações na próxima guia como padrão.
    f. Clique em **Finish**.

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

11. Selecione o nome e execute as seguintes etapas:
    a. Clique em **Editar Política de emissão de reclamação**.
    b. Clique em **Adicionar regra** e clique em **seguinte**.
    c. Especifique um nome para a regra de reclamação.
    d. Selecione **ative Directory** como o armazenamento de atributos.
    e. Selecione o atributo como **User-Principal-Name** e o tipo de reclamação enviada como **Name-ID**.
    f. Clique em **Finish**.
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 etapas a seguir para confirmar se os metadados foram importados com êxito.
    a. Clique com o botão direito do rato na confiança da parte dependente e selecione **Propriedades**.
    b. Certifique-se de que os campos Endpoints, Identificadores e assinatura estão preenchidos.
14. Feche todas as guias do navegador e reabra um navegador para limpar os cookies de sessão existentes ou ativos e faça login novamente.

A funcionalidade de MFA do SnapCenter também pode ser ativada usando APIS REST.

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

Atualizar metadados MFA do AD FS

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

Passos

1. Faça download do arquivo de metadados de federação do AD FS de "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"
2. Copie o arquivo baixado para o servidor SnapCenter para atualizar a configuração 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 guias do navegador e reabra um navegador para limpar os cookies de sessão existentes ou ativos e faça login novamente.

Atualizar os 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 da CA, DR, etc.

Passos

1. No host do AD FS, abra o assistente de gerenciamento do AD FS e execute as seguintes etapas:
   a. Clique em **confiança de parte**.
   b. Clique com o botão direito do Mouse na confiança de quem confia que foi criada para o SnapCenter e clique em **Excluir**.

      O nome definido pelo utilizador da confiança da parte dependente será apresentado.

   c. Habilite a autenticação multifator (MFA).

      "Ativar a autenticação multifator"Consulte .
2. Feche todas as guias do navegador e reabra um navegador para limpar os cookies de sessão existentes ou ativos e faça login novamente.

Desativar a autenticação multifator (MFA)

Passos

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

Gerencie a autenticação multifator (MFA) usando API REST, PowerShell e SCCLI

O login no MFA é compatível com navegador, API REST, PowerShell e SCCLI. O MFA é suportado por um gerenciador de identidade do AD FS. Você pode ativar o MFA, desativar o MFA e configurar o MFA a partir de GUI, API REST, PowerShell e SCCLI.

Configurar o AD FS como OAuth/OIDC

- Configurar o AD FS usando o assistente GUI do Windows*

1. Navegue até **Painel do Gestor do servidor** > **Ferramentas** > **Gestão ADFS**.
2. Navegue até **ADFS** > **grupos de aplicativos**.
   a. Clique com o botão direito do rato em **grupos de aplicações**.
   b. Selecione **Adicionar grupo de aplicativos** e digite **Nome do aplicativo**.
   c. Selecione **aplicação de servidor**.
   d. Clique em **seguinte**.
3. Copiar **Identificador do cliente**.

   Esta é a ID do cliente. .. Adicionar URL de retorno de chamada (URL do servidor SnapCenter) em URL de redirecionamento. .. Clique em **seguinte**.

4. Selecione **Generate shared secret** (gerar segredo partilhado).

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

5. Na página **Summary**, clique em **Next**.
   a. Na página **Complete**, clique em **Close**.
6. Clique com o botão direito no recém-adicionado **Application Group** e selecione **Properties**.
7. Selecione **Adicionar aplicativo** nas Propriedades do aplicativo.
8. Clique em **Adicionar aplicativo**.

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

9. Na página Configurar API da Web, digite o URL do servidor SnapCenter e o identificador do cliente criados na etapa anterior na seção Identificador.
   a. Clique em **Add**.
   b. Clique em **seguinte**.
10. Na página **escolha Política de Controle de Acesso**, selecione a política de controle com base em sua exigência (por exemplo, permitir todos e exigir MFA) e clique em **Avançar**.
11. Na página **Configurar permissão de aplicativo**, por padrão openid é selecionado como um escopo, clique em **Avançar**.
12. Na página **Summary**, clique em **Next**.

    Na página **Complete**, clique em **Close**.

13. Na página **Sample Application Properties**, clique em **OK**.
14. Token JWT emitido por um servidor de autorização (AD FS) e destinado a ser consumido pelo recurso.

    A reivindicação 'aud' ou audiência 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 servidor SnapCenter) e o identificador do cliente foram adicionados corretamente.

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

16. Abra a ferramenta **AD FS Management** localizada no menu **Tools** no canto superior direito do Gerenciador de servidores.
    a. Selecione a pasta **grupos de aplicativos** na barra lateral esquerda.
    b. Selecione a API Web e clique em **edit**.
    c. Ir para a guia regras de transformação de emissão
17. Clique em **Adicionar regra**.
    a. Selecione **Enviar atributos LDAP como reclamações** no menu suspenso modelo de regra de reclamação.
    b. Clique em **seguinte**.
18. Introduza o nome **regra de reclamação**.
    a. Selecione **ative Directory** no menu suspenso Attribute store.
    b. Selecione **User-Principal-Name** no menu suspenso **LDAP Attribute** e **UPN** no menu suspenso o*utgoing Claim Type*.
    c. Clique em **Finish**.

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 reivindicações usando comandos do PowerShell. Esses comandos estão disponíveis em formato de script automatizado. Para obter mais informações, consulte o artigo da KB>.

1. Crie o novo grupo de aplicativos no AD FS usando o seguinte comamnd.

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

   `ClientRoleIdentifier` nome do seu grupo de aplicações

   `redirectURL` URL válido para redirecionamento após autorização

2. Crie o aplicativo AD FS Server 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 a partir da saída dos seguintes comandos porque, ele é mostrado 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 Transform rules.

```
$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 o tempo de expiração do token de acesso

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

Sobre esta tarefa

- Um token de acesso pode ser usado apenas para uma combinação específica de usuário, cliente e recurso. Os tokens de acesso não podem ser revogados e são válidos até sua expiração.
- Por padrão, o tempo de expiração de um token de acesso é de 60 minutos. Este tempo de expiração mínimo é suficiente e dimensionado. Você deve fornecer valor suficiente para evitar qualquer trabalho crítico contínuo dos negócios.

Passo

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

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

Obtenha o token portador do AD FS

Você deve preencher os parâmetros abaixo mencionados em qualquer cliente REST (como Postman) e ele solicita 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 portador.

A validade do token portador é configurável a partir do servidor AD FS por aplicativo e o período de validade padrão é de 60 minutos.

Campo	Valor
Tipo de concessão	Código de autorização
URL de retorno de chamada	Insira o URL base do aplicativo se você não tiver um URL de retorno de chamada.
URL de autenticação	[adfs-domain-name]/adfs/oauth2/autorize
Acesse o URL do token	[adfs-domain-name]/adfs/oauth2/token
ID do cliente	Introduza a ID de cliente do AD FS
Segredo do cliente	Insira o segredo do cliente do AD FS
Âmbito de aplicação	OpenID
Autenticação do cliente	Enviar como cabeçalho AUTH básico
Recurso	Na guia **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 servidor SnapCenter usando PowerShell, SCCLI e API REST

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

Autenticação de CLI de MFA do SnapCenter

No PowerShell e 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>]
```

Depois que o cmdlet acima é executado, uma sessão é criada para que o respetivo usuário execute outros cmdlets SnapCenter.

Autenticação da API REST do SnapCenter MFA

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

Fluxo de trabalho da API REST 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 (API REST do SnapCenter) para executar qualquer operação.

Passos

Para autenticar através do AD FS MFA

1. Configure o CLIENTE REST para chamar o endpoint do AD FS para obter o token de acesso.

   Quando você pressiona o botão para obter um token de acesso para um aplicativo, você será redirecionado para a página SSO do AD FS, onde você deve fornecer suas credenciais do AD e autenticar com 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 de domínio ou domínio/usuário.

2. Na caixa de texto Senha, digite sua senha.
3. Clique em **Log in**.
4. Na seção **Opções de login**, selecione uma opção de autenticação e autentique (dependendo da configuração).
   - Push: Aprove a notificação de envio que é enviada para o telefone.
   - Código QR: Use o aplicativo móvel AUTH Point para digitalizar o código QR e, em seguida, digite o código de verificação mostrado no aplicativo
   - Senha de uso único: Digite a senha de uso único do token.
5. Após a autenticação bem-sucedida, um pop-up será aberto que contém o Access, ID e Atualizar Token.

   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 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.

Ative ou desative a funcionalidade SnapCenter MFA para API REST, CLI e GUI

GUI

Passos

1. Inicie sessão no servidor SnapCenter como Administrador do SnapCenter.
2. Clique em **Configurações** > **Configurações globais** > **Configurações MultiFactorAuthentication(MFA)**
3. Selecione a interface (GUI/RST API/CLI) para ativar ou desativar o login MFA.
   - Interface do PowerShell*

Passos

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

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

   O parâmetro PATH especifica a localização do arquivo xml de metadados MFA do AD FS.

   Habilita o MFA para GUI do SnapCenter, API REST, PowerShell e SCCLI configurados com 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.

SCCLI Interface

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 POST para ativar MFA para GUI, API REST, PowerShell e SCCLI.

Parâmetro	Valor
URL solicitada	/api/4,9/settings/multifactorauthentication
Método HTTP	Post

Solicitar corpo	"IsGuiMFAEnabled": False, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSConfigFilePath": "C: ADFS_metadata.abc.xml"
Corpo de resposta	"IGuiMFAEnabled": False, "ADFSConfigFilePath": NULL, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "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/multifactorauthentication
Método HTTP	Obter
Corpo de resposta	"IGuiMFAEnabled": False, "ADFSConfigFilePath": NULL, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSHostName": "win-adfs-sc49.winscedom2.com"

Instale o servidor SnapCenter no host Windows

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

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

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

Antes de começar

- O host do servidor SnapCenter deve estar atualizado com as atualizações do Windows sem reiniciar o sistema pendente.
- Você deve ter assegurado que o servidor MySQL não está instalado no host onde você pretende instalar o servidor SnapCenter.
- Você deve ter habilitado a depuração do instalador do Windows.

  Consulte o site da Microsoft para obter informações sobre como ativar "Registo do instalador do Windows"o .

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

Passos

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

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

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

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

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

   > O caráter especial "`"%" is not supported in the custom path for the repository database. If you include "%"` no caminho, falha na instalação.

4. Clique em **Instalar agora**.

   Se você tiver especificado quaisquer valores inválidos, as mensagens de erro apropriadas serão exibidas. Você deve reinserir os valores e, em seguida, iniciar a instalação.

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

   No entanto, se você clicar em **Cancelar** quando as operações "SnapCenter Server site Restart" ou "Waiting for SnapCenter Server to start" estiverem sendo executadas, a instalação continuará sem cancelar a operação.

   Os ficheiros de registo estão sempre listados (o mais antigo primeiro) na pasta %temp% do utilizador admin. Se você quiser redirecionar os locais de log, inicie a instalação do servidor SnapCenter a partir do prompt de comando executando:`C:\installer_location\installer_name.exe /log"C:\"`

Registre o produto para habilitar o suporte

Se você é novo nos produtos NetApp e não tem uma conta NetApp existente, deve Registrar o produto para habilitar o suporte.

Passos

1. Depois de 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.comem .
4. Clique em **Eu não sou um Cliente NetApp registrado**.
5. Especifique os seus dados para se registar.
6. Deixe o campo NetApp Reference SN em branco.
7. Selecione **SnapCenter** na lista suspensa linha de produtos.

8. Selecione o fornecedor de faturação.
9. Insira o ID da instância do SnapCenter de 20 dígitos.
10. Clique em **Enviar**.

Instale o servidor SnapCenter no host Linux

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

Antes de começar

- Se você quiser instalar o servidor SnapCenter usando um usuário não-root que não tenha Privileges suficiente para instalar o SnapCenter, obtenha o arquivo de checksum de sudoers no site de suporte da NetApp. Você deve usar o arquivo de checksum apropriado baseado na versão Linux.
- Durante a instalação do runtime .NET, se a instalação não conseguir resolver as dependências da biblioteca *libicu*, então instale *libicu* executando o comando: `yum install -y libicu`
- Se a instalação do servidor SnapCenter falhar devido à não disponibilidade de *Perl*, então instale *Perl* executando o comando: `yum install -y perl`
- Se o pacote sudo não estiver disponível no SUSE Linux, instale o pacote sudo para evitar falha de autenticação.
- Para o SUSE Linux, configure o nome do host para evitar a falha de instalação.
- Verifique o status seguro do Linux executando o comando `sestatus`. Se o status *SELinux* estiver "ativado" e o modo *atual* estiver "aplicando", 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 a partir do 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 novamente o comando após instalar o servidor SnapCenter.
    - Se o comando criar *my-nginx.PP*, execute o comando para tornar o pacote de políticas ativo: `sudo semodule -i my-nginx.pp`
  - O caminho usado para o diretório PID do MySQL é */var/opt/mysqld*. Execute os seguintes comandos para definir as permissões para a 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 MySQL é */install_DIR/NetApp/SnapCenter/SnapManagerWeb/Repositório/MySQL/*. Execute os seguintes comandos para definir as permissões para o diretório de dados 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 servidor SnapCenter é instalado no host Linux, serviços de terceiros como MySQL, RabbitMq, Errlang são instalados. Você não deve desinstalá-los.
- O servidor SnapCenter instalado no host Linux não suporta:
  - Alta disponibilidade
  - Plug-ins do Windows
  - Ative Directory (suporta apenas os utilizadores locais, tanto o utilizador raiz como o utilizador não-raiz com creds)
  - Autenticação baseada em chave para fazer login no SnapCenter

Passos

1. Faça o download do seguinte de "Site de suporte da NetApp" para */home Directory*.
   - Pacote de instalação do servidor SnapCenter - **SnapCenter-linux-server-(el8/el9/sles15).bin**
   - Arquivo de chave pública - **SnapCenter_public_key.pub**
   - Respetivo arquivo de assinatura - **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 usuários que não sejam root, adicione o conteúdo visualizado especificado em **SnapCenter_Server_checksum_(el8/el9/sles15).txt** disponível junto com o instalador .bin.
4. Atribua a permissão executar para o instalador .bin.
   `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. Execute uma das ações para instalar o servidor SnapCenter.

Se você quiser executar…	Faça isso…
Instalação interativa	`./snapcenter-linux-server-(el8/el9/sles15).bin` Ser-lhe-á pedido que introduza os seguintes detalhes: • A porta externa do webapp usada para acessar o servidor SnapCenter fora do host Linux. O valor padrão é 8146. • O usuário do servidor SnapCenter que instalará o servidor SnapCenter. • 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 registos serão armazenados em */var/opt/SnapCenter/logs*. Parâmetros a serem passados para a instalação do servidor SnapCenter: • DWEBAPP_EXTERNAL_port: Porta externa webapp usada para acessar o servidor SnapCenter fora do host Linux. O valor padrão é 8146. • DWEBAPP_INTERNAL_port: Porta interna do webapp usada para acessar o servidor SnapCenter dentro do 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 servidor SnapCenter que instalará o servidor SnapCenter. 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 esse parâmetro, os logs serão exibidos no console e também armazenados no arquivo de log padrão.

O que se segue?

- Se o status *SELinux* estiver "habilitado" e o modo *atual* estiver "impondo", o serviço **nginx** não será iniciado. Você deve executar os seguintes comandos:
  a. Vá para o diretório inicial.
  b. Executar o comando: `journalctl -x|grep nginx`.
  c. Se a porta interna do Webapp (8147) não tiver permissão padrão, execute os seguintes comandos:
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. Executar `setsebool -P httpd_can_network_connect on`
- DSELINUX: Se o status *SELinux* estiver "habilitado", o *current mode* está "impondo", e você executou os comandos mencionados na seção antes de começar, você deve especificar esse parâmetro e atribuir o valor como 1. O valor padrão é 0.
- DUPGRADE: O valor padrão é 0. Especifique este parâmetro e seu valor como qualquer inteiro diferente de 0 para atualizar o servidor SnapCenter.

Registre o produto para habilitar o suporte

Se você é novo no NetApp e não tem uma conta NetApp existente, deve Registrar o produto para habilitar o suporte.

Passos

1. Depois de 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.comem .
4. Clique em **Eu não sou um Cliente NetApp registrado**.
5. Especifique os seus dados para se registar.
6. Deixe o campo NetApp Reference SN em branco.
7. Selecione **SnapCenter** na lista suspensa linha de produtos.
8. Selecione o fornecedor de faturação.
9. Insira o ID da instância do SnapCenter de 20 dígitos.
10. Clique em **Enviar**.

Faça login no SnapCenter usando a autorização RBAC

O SnapCenter é compatível com controles de acesso baseados em função (RBAC). O administrador do SnapCenter atribui funções e recursos por meio do SnapCenter RBAC a um usuário no grupo de trabalho ou diretório ativo ou a grupos no diretório ativo. O usuário RBAC agora pode fazer login no SnapCenter com as funções atribuídas.

Antes de começar

- Você deve ativar o Serviço de ativação do processo do Windows (WAS) no Gerenciador do Windows Server.
- Se pretender utilizar o Internet Explorer como browser para iniciar sessão no servidor SnapCenter, deve certificar-se de que o modo protegido no Internet Explorer está desativado.
- Se o servidor SnapCenter estiver instalado no host Linux, você deve fazer login usando a conta de usuário que foi usada para instalar o servidor SnapCenter.

Sobre esta tarefa

Durante a instalação, o assistente de instalação do servidor SnapCenter 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 navegador da Web, fechar apenas a guia do navegador do SnapCenter não fará o logout do SnapCenter. Para terminar sua conexão com o SnapCenter, você deve sair do SnapCenter clicando no botão **Sair** ou fechando todo o navegador da Web.

Prática recomendada: por motivos de segurança, recomenda-se que não ative o seu navegador para guardar a sua palavra-passe do SnapCenter.

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

Para a implantação de alta disponibilidade (HA), você deve acessar o SnapCenter usando o IP *https://Virtual_Cluster_IP_or_FQDN:8146*. do cluster virtual Se você não vir a IU do SnapCenter ao navegar para *https://Virtual_Cluster_IP_or_FQDN:8146* no Internet Explorer (IE), você deve adicionar o endereço IP do cluster virtual ou FQDN como um site confiável no IE em cada host de plug-in ou desativar a Segurança aprimorada do IE em cada host de plug-in. Para obter mais informações, "Não é possível acessar o endereço IP do cluster a partir da rede externa"consulte .

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 sido alterados com cada versão do SnapCenter. O "Guia de referência de cmdlet do software SnapCenter" tem os detalhes.

Se estiver a iniciar sessão no SnapCenter pela primeira vez, tem de iniciar sessão utilizando 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 do URL fornecido no final da instalação, ou a partir do URL fornecido pelo administrador do SnapCenter.
2. Introduza as credenciais do utilizador.

Para especificar o seguinte…	Use um destes formatos…
Administrador de domínio	• NetBIOS/nome de usuário • Sufixo UPN Por exemplo, NetApp.com • Nome de usuário do domínio
Administrador local	Nome de utilizador

3. Se lhe for atribuída mais de uma função, na caixa função, selecione a função que pretende utilizar para

esta sessão de início de sessão.

Seu usuário atual e sua função associada são mostrados no canto superior direito do SnapCenter depois que você estiver conetado.

Resultado

É apresentada a página Painel de instrumentos.

Se o log falhar com o erro de que o site não pode ser alcançado, você deve mapear o certificado SSL para o SnapCenter. "Saiba mais"

Depois de terminar

Depois de efetuar login no servidor SnapCenter como usuário RBAC pela primeira vez, atualize a lista de recursos.

Se você tiver domínios não confiáveis do ative Directory que deseja que o SnapCenter ofereça suporte, Registre esses domínios no SnapCenter antes de configurar as funções dos usuários em domínios não confiáveis. "Saiba mais".

Se você quiser adicionar o host do plug-in no SnapCenter em execução no host Linux, você deve obter o arquivo de checksum do 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.

Faça login no SnapCenter usando autenticação multifator (MFA)

O servidor SnapCenter suporta MFA para conta de domínio, que faz parte do diretório ativo.

Antes de começar

Você deve ter habilitado o MFA. Para obter informações sobre como ativar o MFA, consulte "Ativar a autenticação multifator"

Sobre esta tarefa

- Apenas o FQDN é suportado
- Os usuários de grupos de trabalho e entre domínios não podem fazer login usando MFA

Passos

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

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

   - Se o nome de usuário ou senha é válido

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

   - Se você excedeu o máximo de tentativas permitidas que foi definido no AD

- Se o AD e o AD FS estão ativos e em execução

Modifique o tempo limite padrão da sessão da GUI 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 um recurso de segurança, após um período padrão de 15 minutos de inatividade, o SnapCenter avisa que você será desconetado da sessão da GUI em 5 minutos. Por padrão, o SnapCenter faz o logout da sessão da GUI após 20 minutos de inatividade e você deve fazer login novamente.

Passos

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

Proteja o servidor web SnapCenter desativando o SSL 3,0

Para fins de segurança, você deve desativar o protocolo SSL (Secure Socket Layer) 3,0 no Microsoft IIS se ele estiver ativado no servidor da Web SnapCenter.

Há falhas no protocolo SSL 3,0 que um invasor pode usar para causar falhas de conexão, ou para executar ataques man-in-the-middle e observar o tráfego de criptografia entre seu site e seus visitantes.

Passos

1. Para iniciar o Editor de Registro no host do servidor web do SnapCenter, clique em **Iniciar** > **Executar** e, em seguida, digite regedit.
2. No Editor de 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 ativado 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, em seguida, nomeie o servidor de chaves.
     ii. Com a nova chave de servidor selecionada, clique em **Edit** > **New** > **DWORD**.
     iii. Nomeie o novo DWORD habilitado e insira 0 como o valor.
3. Feche o Editor de Registro.

Configurar o certificado CA para o host Windows

Gerar arquivo CSR do 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 a CSR gerada. O certificado terá uma chave privada associada a ele.

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

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

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

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

Para configurações de cluster, o nome do cluster (FQDN de cluster virtual) e os respetivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome alternativo (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados CA

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 **Yes**, importe a chave privada e clique em **Next**.
Importar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

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

7. Repita o passo 5 para a pasta "Pessoal".

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia 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 **thumbprint**.
   d. Copie os carateres 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

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.

Configure o certificado CA com os serviços de plug-in do host do Windows

Você deve configurar o certificado CA com os serviços de plug-in host do Windows para ativar o certificado digital instalado.

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, 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"
```

Configure o 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 servidor Windows em que o SnapCenter está instalado.
2. No painel de navegação esquerdo, clique em **Connections** (ligações).
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**, clique em **ligações**.
6. Na página ligações, selecione **encadernação para https**.
7. Clique em **Editar**.
8. Na lista suspensa certificado SSL, selecione o certificado SSL recentemente importado.
9. Clique em **OK**.

> O site do Agendador de SnapCenter (porta padrão: 8154, HTTPS) é configurado com certificado autoassinado. Esta porta está se comunicando dentro do host do servidor SnapCenter e não é obrigatório configurar com um certificado de CA. No entanto, se o seu ambiente exigir que você use um certificado de CA, repita as etapas de 5 a 9 usando o site Agendador de SnapCenter.

> Se o certificado da CA recentemente implantado não estiver listado no menu suspenso, verifique se o certificado da CA está associado à chave privada.

> Certifique-se de que o certificado é adicionado usando o seguinte caminho: **Raiz da consola > certificados – computador local > autoridades de certificação raiz fidedignas > certificados**.

Ativar certificados de CA para SnapCenter

Você deve configurar os certificados da CA e ativar a validação do certificado da CA para o servidor SnapCenter.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet Set-SmCertificateSettings.
- Você pode exibir o status do certificado para o servidor SnapCenter 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*. Em alternativa, pode consultar a "Guia de referência de 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 de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- * * Indica que não há certificado CA habilitado ou atribuído ao host do plug-in.
- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da 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 são concluídas com êxito.

Configure o certificado CA para o host Linux

Depois de instalar o servidor SnapCenter no Linux, o instalador cria o certificado autoassinado. Se você quiser usar o certificado da CA, configure os certificados para proxy reverso nginx, log de auditoria e serviços SnapCenter.

Configure o certificado nginx

Passos

1. Navegue para */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. Recarregar nginx: `$nginx -s reload`

Configurar o 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 respetivamente.

   Apenas o formato *.pfx* é suportado para o certificado de registo de auditoria.

3. Salve e feche o arquivo.
4. Reinicie o serviço **snapmanagerweb**: `$ systemctl restart snapmanagerweb`

Configurar o certificado de serviços 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 e a senha do certificado da CA, respetivamente.

   Apenas o formato *.pfx* é suportado para o certificado de serviços SnapCenter.

3. Salve e feche os arquivos.
4. Reinicie todos os serviços.
   - `$ systemctl restart snapmanagerweb`
   - `$ systemctl restart smcore`
   - `$ systemctl restart scheduler`

Configure e ative 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 servidor SnapCenter 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 CA deve suportar autenticação de servidor e autenticação de cliente.
- Você deve ter um certificado CA com chave privada e detalhes de impressão digital.
- Você deve ter habilitado a configuração SSL unidirecional.

  Para obter mais detalhes, consulte "Configurar a seção certificado CA."

- Você deve ter habilitado a comunicação SSL bidirecional em todos os hosts de plug-in e no servidor SnapCenter.

  O ambiente com alguns hosts ou servidor não habilitado para comunicação SSL bidirecional não é suportado.

Passos

1. Para vincular a porta, execute as etapas a seguir no host do servidor SnapCenter para a porta 8146 do servidor Web do SnapCenter IIS (padrão) e novamente para a porta 8145 do SMCore (padrão) usando comandos do PowerShell.

   a. Remova a vinculação de porta de certificado auto-assinada do SnapCenter existente usando o seguinte comando 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 com o servidor SnapCenter e a 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 ao certificado da CA, adicione o usuário padrão do servidor Web IIS "**SnapCenter**" do SnapCenter na lista de permissões do certificado executando as etapas a seguir para acessar o certificado da CA recém-adquirida.
   a. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove SnapIn**.
   b. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
   c. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
   d. Clique em **raiz da consola** > **certificados – computador local** > **Pessoal** > **certificados**.
   e. Selecione o certificado SnapCenter.
   f. Para iniciar o assistente 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 **Add**, no assistente Select Users and Groups (Selecionar usuários e grupos) altere o local para o nome do computador local (mais importante na hierarquia)
   h. Adicione o usuário do AppPool/SnapCenter do IIS, dê permissões de controle total.
3. Para **permissão IIS de certificado CA**, adicione a nova entrada de chaves de Registro DWORD no servidor SnapCenter a partir do seguinte caminho:

   No editor de Registro do Windows, percorra para o caminho abaixo mencionado,

   ```
   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
   ```

Configure o plug-in do SnapCenter para comunicação SSL bidirecional

Você deve configurar o plug-in do SnapCenter para comunicação SSL bidirecional usando comandos do PowerShell.

Antes de começar

Verifique se a impressão digital do certificado CA está disponível.

Passos

1. Para vincular a porta, execute as seguintes ações no host de plug-in do Windows para a porta SMCore 8145 (padrão).

a. Remova a vinculação de porta de certificado auto-assinada do SnapCenter existente usando o seguinte comando 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 com a 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
```

Ative a comunicação SSL bidirecional no host Windows

Você pode habilitar a comunicação SSL bidirecional para proteger a comunicação mútua entre o servidor SnapCenter 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 ativar a comunicação SSL bidirecional, execute os seguintes comandos no servidor SnapCenter para os plug-ins, 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 PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

Desative a comunicação SSL bidirecional

Você pode desativar 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 desativa a comunicação SSL bidirecional, o certificado da CA e sua configuração não são removidos.
- Para adicionar um novo host ao servidor SnapCenter, você deve desativar o SSL bidirecional para todos os hosts de plug-in.
- NLB e F5 não são suportados.

Passos

1. Para desativar a comunicação SSL bidirecional, execute os seguintes comandos no servidor SnapCenter 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 PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

Configure e habilite a 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 servidor SnapCenter 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 servidor SnapCenter.

Passos

1. Copiar **certificate.pem** para */etc/pki/CA-trust/source/ancors/*.
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 servidor SnapCenter.
6. Atualize os valores das seguintes chaves em **SnapManager.Web.UI.dll.config** localizado em _ /<installation path>/NetApp/SnapCenter/SnapManagerWeb_ e **SMCoreServiceHost.dll.config** localizado em */<installation path>/NetApp/SnapCenter/SMCore*.
   - <add key="SERVICE_CERTIFICATE_PATH" value="<path of certificate.pfx>" />
   - <add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>
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 o keystore SPL e alias.
    a. Recupere a senha padrão do keystore SPL atribuída à chave **SPL_KEYSTORE_PASS** no arquivo de propriedades SPL.
    b. Altere a senha do keystore.
       `keytool -storepasswd -keystore keystore.jks`
    c. Altere a senha para 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 plug-in, adicione os certificados raiz e intermediários 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 no 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`

Ative a comunicação SSL no host Linux

Você pode habilitar a comunicação SSL bidirecional para proteger a comunicação mútua entre o servidor SnapCenter no host Linux e os plug-ins usando comandos do PowerShell.

Passo

1. Execute o seguinte para ativar a comunicação SSL unidirecional.
   a. Entre na GUI do SnapCenter.
   b. Clique em **Configurações** > **Configurações globais** e selecione **Ativar validação de certificado no servidor SnapCenter**.
   c. Clique em **hosts** > **hosts gerenciados** e selecione o host do plug-in para o qual você deseja habilitar o SSL unidirecional.
   d. Clique em e, em seguida, clique em **Ativar validação de certificado**.
2. Ative a comunicação SSL bidirecional a partir do host Linux do servidor SnapCenter.
   - `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 autenticação baseada em certificado

Exportar certificados de autoridade de certificação (CA) do servidor SnapCenter

Você deve exportar os certificados de CA do servidor SnapCenter para os hosts de plug-

in usando o MMC (console de gerenciamento da Microsoft).

Antes de começar

Você deve ter configurado o SSL bidirecional.

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela certificados Snap-in, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados - computador local** > **Pessoal** > **certificados**.
5. Clique com o botão direito do rato no certificado CA adquirido, que é utilizado para o servidor SnapCenter 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 exporte a chave privada** e, em seguida, clique em **seguinte**.
Exportar formato de ficheiro	Clique em **seguinte**.
Nome do ficheiro	Clique em **Procurar** e especifique o caminho do arquivo para salvar o certificado e clique em **Avançar**.
Concluir o Assistente de exportação de certificados	Revise o resumo e clique em **Finish** para iniciar a exportação.

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

Importar certificado de autoridade de certificação (CA) para os hosts de plug-in do Windows

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela certificados Snap-in, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados - computador local** > **Pessoal** > **certificados**.
5. Clique com o botão direito 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 **seguinte**.
Ficheiro a importar	Selecione o certificado do servidor SnapCenter que termina com a extensão .cer.
Armazenamento de certificados	Clique em **seguinte**.
Concluir o Assistente de exportação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

Importe o certificado CA para os plug-ins do host UNIX e configure certificados raiz ou intermediários para o armazenamento de confiança SPL

Importar certificado CA para os hosts de plug-in UNIX

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

Sobre esta tarefa

- Você pode gerenciar a senha do armazenamento de chaves SPL e o alias do par de chaves assinadas CA em uso.
- A senha para o keystore SPL e para toda a senha de alias associada da chave privada deve ser a mesma.

Passos

1. Você pode recuperar a senha padrão do keystore SPL do arquivo de propriedade SPL. É o valor correspondente à chave `SPL_KEYSTORE_PASS`.
2. Altere a senha do keystore:
   `$ keytool -storepasswd -keystore keystore.jks`
3. Altere a senha para 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 no `spl.properties` arquivo.
5. Reinicie o serviço depois de alterar a senha.

Configure certificados raiz ou intermediários para o armazenamento de confiança SPL

Você deve configurar os certificados raiz ou intermediários para o SPL Trust-store. Você deve adicionar o certificado de CA raiz e, em seguida, os certificados de CA intermediários.

Passos

1. Navegue até a pasta que contém o keystore SPL: `/var/opt/snapcenter/spl/etc`.

2. Localize o arquivo `keystore.jks`.
3. Liste 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 depois de configurar os certificados raiz ou intermédios para o armazenamento de confiança SPL.

Configure o par de chaves assinadas da CA para o armazenamento de confiança SPL

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança 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. Liste 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. Liste os certificados adicionados no keystore.
   `$ keytool -list -v -keystore keystore.jks`
6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

   A senha padrão do keystore SPL é o valor da chave SPL_KEYSTORE_PASS no `spl.properties` arquivo.

   `$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
8. Se o nome do alias no certificado da CA for longo e contiver espaço ou carateres 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 a partir do keystore localizado no `spl.properties` arquivo. Atualize este valor com a chave SPL_CERTIFICATE_ALIAS.
10. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança SPL.

Ativar autenticação baseada em certificado

Para habilitar a autenticação baseada em certificado para o servidor SnapCenter e os hosts de plug-in do Windows, execute o cmdlet do PowerShell a seguir. Para os hosts de

plug-in Linux, a autenticação baseada em certificado será ativada quando você ativar o SSL bidirecional.

- Para ativar a autenticação baseada em certificado de cliente:

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

- Para desativar a autenticação baseada em certificado de cliente:

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

Exportar certificados SnapCenter

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snap-in**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **minha conta de usuário** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados - Utilizador atual** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato 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, exporte a chave privada** e clique em **Avançar**.
Exportar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Ficheiro a exportar	Especifique um nome de arquivo para o certificado exportado (você deve usar .pfx) e clique em **Next**.
Concluir o Assistente de exportação de certificados	Revise o resumo e clique em **Finish** para iniciar a exportação.

Resultado

Os certificados são exportados no formato .pfx.

Configure o ative Directory, LDAP e LDAPS

Registre domínios não confiáveis do ative Directory

Você deve Registrar o ative Directory com o servidor SnapCenter para gerenciar hosts, usuários e grupos de vários domínios não confiáveis do ative Directory.

Antes de começar

Protocolos LDAP e LDAPS

- Você pode Registrar os domínios de diretório ativo não confiáveis usando o protocolo LDAP ou LDAPS.
- Você deve ter habilitado a comunicação bidirecional entre os hosts do plug-in e o servidor SnapCenter.
- A resolução DNS deve ser configurada do servidor SnapCenter para os hosts plug-in e vice-versa.

Protocolo LDAP

- O nome de domínio totalmente qualificado (FQDN) deve ser resolvido a partir do servidor SnapCenter.

  Você pode Registrar um domínio não confiável com o FQDN. Se o FQDN não for resolvido a partir do servidor SnapCenter, você pode se Registrar com um endereço IP do controlador de domínio e isso deve ser resolvido a partir do servidor SnapCenter.

Protocolo LDAPS

- Os certificados CA são necessários para que o LDAPS forneça criptografia de ponta a ponta durante a comunicação do diretório ativo.

  "Configure o certificado de cliente CA para LDAPS"

- Os nomes de host do controlador de domínio (DCHostName) devem ser acessíveis a partir do servidor SnapCenter.

Sobre esta tarefa

- Você pode usar a interface de usuário do SnapCenter, cmdlets do PowerShell ou 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 selecionar **LDAP**, especifique as informações necessárias para registar o domínio não fidedigno 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 domínio FQDN não for resolvido a partir do servidor SnapCenter, especifique um ou mais endereços IP do controlador de domínio. Para obter mais informações, "Adicione IP do controlador de domínio para domínio não confiável da GUI"consulte .

b. Se selecionar **LDAPS**, especifique as informações necessárias para registar o domínio não fidedigno 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 controlador de domínio	Especifique um ou mais nomes de controlador de domínio e clique em **resolver**.
Endereços IP do controlador de domínio	Se os nomes do controlador de domínio não forem solucionáveis a partir do servidor SnapCenter, você deve corrigir as resoluções DNS.

6. Clique em **OK**.

Configure o certificado de cliente CA para LDAPS

Você deve configurar o certificado de cliente CA para LDAPS no servidor SnapCenter quando o LDAPS do ative Directory do Windows estiver configurado com os certificados de CA.

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 **Browse**, selecione o *root Certificate* e clique em **Next**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

7. Repita os passos 5 e 6 para os certificados intermédios.

Configurar alta disponibilidade

Configurar servidores SnapCenter para alta disponibilidade

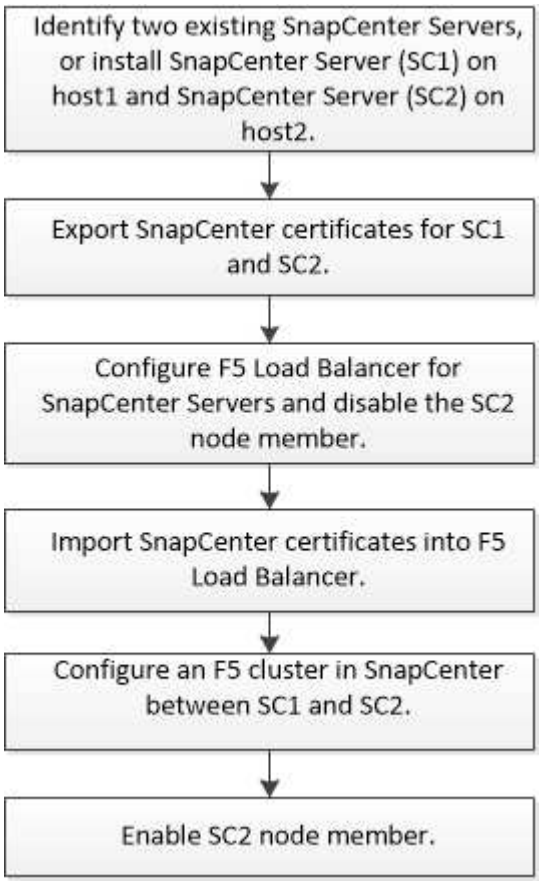
Para oferecer suporte a alta disponibilidade (HA) no SnapCenter executado no Windows ou no Linux, você pode instalar o balanceador de carga F5. O F5 permite que o servidor SnapCenter suporte configurações ativo-passivo em até dois hosts que estão no mesmo local. Para usar o balanceador de carga F5 no 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 o SnapCenter High Availability. Você deve configurar manualmente o NLB fora da instalação do SnapCenter para alta disponibilidade.

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

Configure a alta disponibilidade usando o F5

A imagem do fluxo de trabalho lista as etapas para configurar os servidores SnapCenter para alta disponibilidade usando o balanceador de carga F5. Para obter instruções detalhadas, "Como configurar servidores SnapCenter para alta disponibilidade usando o balanceador de carga F5" consulte .



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

- Add-SmServerCluster
- Add-SmServer
- Remover-SmServerCluster

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

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 servidores SnapCenter e houver também uma sessão do 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 parcialmente resolvido pelo NLB ou host F5 e se o host SnapCenter não conseguir entrar em Contato com esse host, a página do host SnapCenter alternará entre hosts inativos e o estado em execução com frequência. Para resolver esse problema, você deve garantir que ambos os hosts do SnapCenter

sejam capazes de resolver o host no NLB ou no host F5.

- Os comandos SnapCenter para configurações de MFA devem ser executados em todos os hosts. A configuração do grupo dependente deve ser feita no servidor AD FS (Serviços de Federação do ative Directory) usando os detalhes do cluster F5. O acesso à IU 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 de log de auditoria no host passivo F5 quando ele se tornar ativo.

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

Você pode configurar o balanceamento de carga de rede (NLB) para configurar o SnapCenter High Availability. Você deve configurar manualmente o NLB fora da instalação do SnapCenter para alta disponibilidade.

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

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

Você pode configurar o ambiente de SnapCenter de alta disponibilidade no 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 IP de sobreposição virtual privada na AWS. Para obter informações, "Configurar IP de sobreposição virtual privada" consulte .
2. Prepare seu host Windows
   a. Força IPv4 a ser priorizada acima de 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 podem ser resolvidos via DNS ou através da configuração de host local para os endereços IPv4.
   c. Certifique-se de que não tem um proxy do sistema configurado.
   d. Certifique-se de que a palavra-passe de administrador seja a mesma no Windows Server quando utilizar uma configuração sem um ative Directory e que os servidores não estejam num domínio.
   e. Adicione IP virtual em ambos os servidores Windows.
3. Crie o cluster SnapCenter.
   a. Inicie o PowerShell e conete-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 endpoint IP privado virtual fique indisponível, monitorado pelo AWS CloudWatch. Para obter informações, "Crie uma função do Lambda" consulte .
5. Crie um monitor no CloudWatch para monitorar a disponibilidade do endpoint do SnapCenter. Um alarme é configurado para acionar uma função do Lambda se o endpoint estiver inacessível. A função do Lambda ajusta a tabela de roteamento para redirecionar o tráfego para o servidor SnapCenter ativo. Para obter informações, "Crie canários sintéticos" consulte .
6. Implemente o fluxo de trabalho usando uma função de etapa como alternativa ao monitoramento do CloudWatch, fornecendo tempos de failover menores. O fluxo de trabalho inclui uma função de sonda do Lambda para testar o URL do SnapCenter, uma tabela do DynamoDB para armazenar contagens de falhas e a própria função Etapa.
   a. Use uma função lambda para verificar a URL do SnapCenter. Para obter informações, "Crie a função Lambda" consulte .
   b. Crie uma tabela do DynamoDB para armazenar a contagem de falhas entre duas iterações de função de passo. Para obter informações, "Comece a usar a tabela DynamoDB" consulte .
   c. Crie a função Step (passo). Para obter informações, "Documentação da função de passos" consulte .
   d. Teste uma única etapa.
   e. Teste a função completa.
   f. Crie a função do IAM e ajuste as permissões para poder executar a função do Lambda.
   g. Criar agendamento para acionar a função Step. Para obter informações, "Usando o Amazon EventBridge Scheduler para iniciar uma função de passo" consulte .

Configure a alta disponibilidade usando o balanceador de carga do Azure

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

Passos

1. Crie máquinas virtuais em um conjunto de escala usando o portal do Azure. O conjunto de escala de máquina virtual do Azure permite criar e gerenciar um grupo de máquinas virtuais balanceadas de carga. O número de instâncias de máquina virtual pode aumentar ou diminuir automaticamente em resposta à demanda ou a um cronograma definido. Para obter informações, "Crie máquinas virtuais em um conjunto de escala usando o portal do Azure" consulte .
2. Depois de configurar as máquinas virtuais, faça login em cada máquina virtual no VM Set e instale o servidor SnapCenter 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 sua configuração do SnapCenter HA de balanceamento de carga de rede (NLB) para usar o balanceador de carga F5.

Passos

1. Configurar servidores SnapCenter para alta disponibilidade usando o F5. "Saiba mais".
2. No host do servidor SnapCenter, inicie o PowerShell.
3. Inicie uma sessão usando o cmdlet Open-SmConnection e insira suas credenciais.
4. Atualize o servidor SnapCenter 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Alta disponibilidade para o repositório SnapCenter MySQL

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

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 slave então se torna o repositório master. O SnapCenter também dá suporte à replicação reversa, que é ativada somente durante o failover.

Para usar o recurso de alta disponibilidade (HA) do MySQL, você deve 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 se juntar ao 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

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

- NLB e MySQL HA não são suportados além de dois nós.
- Mudar de uma instalação autônoma do SnapCenter para uma instalação NLB ou vice-versa e mudar de uma configuração autônoma do MySQL para o MySQL HA não são suportados.
- O failover automático não é suportado se os dados do repositório secundário não forem sincronizados com os dados do repositório principal.

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

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

  Se o failover acontecer porque o servidor MySQL ou o servidor SnapCenter estão inoperantes, os trabalhos que estão em execução podem falhar. Após o failover para o segundo nó, todos os trabalhos subsequentes são executados com êxito.

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

Configurar controles de acesso baseados em função (RBAC)

Adicione um usuário ou grupo e atribua funções e ativos

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

Antes de começar

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

  Você pode incluir apenas os seguintes carateres especiais em nomes de usuário e nomes de grupo: Espaço ( ), hífen (-), sublinhado (_) e dois pontos (:).

- O SnapCenter inclui várias funções predefinidas.

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

- Os usuários DE ANÚNCIOS e grupos de AD adicionados ao RBAC do SnapCenter devem ter a permissão DE LEITURA no contentor usuários e no contentor computadores no ative Directory.
- Depois de atribuir uma função a um usuário ou grupo que contenha as permissões apropriadas, você deve atribuir o acesso do usuário aos ativos do SnapCenter, como hosts e conexões de armazenamento.

  Isso permite que os usuários executem as ações para as quais eles têm permissões nos ativos que são 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
Proteger recursos	host, política
Backup	host, grupo de recursos, política
Restaurar	host, grupo de recursos
Clone	host, grupo de recursos, política
Ciclo de vida do clone	host
Crie um Grupo de recursos	host

- 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, atribua a conexão de armazenamento para o volume de origem e destino ao usuário que executa a operação.

  Você deve adicionar ativos antes de atribuir acesso aos usuários.

Se você estiver usando o plug-in do SnapCenter para funções do VMware vSphere para proteger VMs, VMDKs ou datastores, use a GUI do VMware vSphere para adicionar um usuário do vCenter a uma função do SnapCenter Plug-in para VMware vSphere. Para obter informações sobre as funções do VMware vSphere, "Funções predefinidas empacotadas com o plug-in SnapCenter para VMware vSphere" consulte .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **usuários e acesse** > * *.
3. Na página Adicionar usuários/grupos do ative 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 conetado. Tem de registar o domínio não fidedigno na na página **Definições** > **Definições globais** > **Definições de domínio**.
Tipo	Selecione Usuário ou Grupo O SnapCenter suporta apenas o grupo de segurança e não o grupo de distribuição.
Nome de utilizador	a. Digite o nome de usuário parcial e clique em **Add**. O nome de usuário diferencia maiúsculas de minúsculas. b. Selecione o nome de utilizador na lista de pesquisa. Quando você adiciona usuários de um domínio diferente ou de um domínio não confiável, você deve digitar o nome de usuário totalmente porque 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 deseja adicionar o usuário.

4. Clique em **Assign** e, em seguida, na página Assign Assets (atribuir ativos):
   a. Selecione o tipo de ativo na lista suspensa **Ativo**.
   b. Na tabela Ativo, selecione o ativo.

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

c. Repita este 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 recursos.

Crie uma função

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

Você deve ter feito login como a função "SnapCenterAdmin".

Passos

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

Você pode incluir apenas os seguintes carateres especiais em nomes de usuário e nomes de grupo: Espaço ( ), hífen (-), sublinhado (_) e dois pontos (:).

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

Você deve desmarcar essa opção se não quiser que os membros dessa função vejam objetos aos quais outros membros são atribuídos.

Quando essa opção está ativada, a atribuição de acesso aos usuários a objetos ou recursos não é necessária se os usuários pertencerem à mesma função que o usuário que criou os objetos ou recursos.

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

Adicione uma função ONTAP RBAC usando comandos de login de segurança

Use os comandos de login de segurança para adicionar uma função RBAC do ONTAP quando seus sistemas de storage estiverem executando o Clustered ONTAP.

Antes de começar

- Antes de criar uma função RBAC do ONTAP para sistemas de storage que executam o Clustered ONTAP, é necessário identificar o seguinte:
  - A tarefa (ou tarefas) que você deseja executar
  - O Privileges necessário para executar essas tarefas

- A configuração de uma função RBAC exige que você execute as seguintes ações:
  - Conceda Privileges aos comandos e/ou diretórios de comando.

    Existem dois níveis de acesso para cada diretório de comando/comando: All-Access e somente leitura.

  Você deve sempre atribuir primeiro o All-Access Privileges.

  - Atribua funções aos usuários.
  - Varie a configuração dependendo se os plug-ins do SnapCenter estão conetados ao IP do administrador de cluster para todo o cluster ou diretamente conetados a um SVM no cluster.

Sobre esta tarefa

Para simplificar a configuração dessas funções em sistemas de storage, você pode usar a ferramenta Criador de usuários do RBAC para Data ONTAP, publicada no Fórum de Comunidades do NetApp.

Esta ferramenta lida automaticamente com a configuração correta do ONTAP Privileges. Por exemplo, a ferramenta Criador de Usuário RBAC para Data ONTAP adiciona automaticamente o Privileges na ordem correta para que o Privileges de Acesso total apareça primeiro. Se você adicionar primeiro o Privileges somente leitura e depois adicionar o Privileges All-Access, o ONTAP marca o Privileges All-Access como duplicatas e os ignora.

> Se você atualizar mais tarde o SnapCenter ou o ONTAP, execute novamente a ferramenta Criador de usuários do RBAC para Data ONTAP para atualizar as funções de usuário criadas anteriormente. As funções de usuário criadas para uma versão anterior do SnapCenter ou do ONTAP não funcionam corretamente com versões atualizadas. Quando você executa novamente a ferramenta, ela manipula automaticamente a atualização. Você não precisa recriar os papéis.

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

> Para consistência, a documentação do SnapCenter refere-se às funções como usando o Privileges. A GUI do OnCommand System Manager usa o termo *attribute* em vez de *Privilege*. Ao configurar funções RBAC do ONTAP, esses dois termos significam a mesma coisa.

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 isso em branco, o padrão será administrador do cluster.
   - role_name é o nome que você especifica para a função.
   - Comando é a capacidade ONTAP.

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

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

atribuir permissões"consulte .

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.
   - <password> é a sua palavra-passe. Se você não especificar uma senha, o sistema solicitará uma.
   - SVM_name é o nome do SVM.

3. Atribua a função ao utilizador introduzindo 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 modificar 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.
   - <password> é a sua palavra-passe. 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.

Criar funções do SVM com Privileges mínimo

Há vários comandos de CLI do ONTAP que você deve executar ao criar uma função para um novo usuário do 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 storage, crie uma função e atribua todas as permissões à função.

```
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 esse usuário.

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

3. Desbloquear o utilizador.

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

Comandos CLI do ONTAP para criar funções SVM e atribuir permissões

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

> A partir do 5,0, os usuários de administração do vserver só são suportados com APIS REST. Se você quiser criar funções usando um administrador que não seja vserver, use o ZAPI.

- `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 de cluster do ONTAP com Privileges mínimo

Você deve criar uma função de cluster do ONTAP com Privileges mínimo para que você não precise usar a função de administrador do ONTAP para executar operações no SnapCenter. Você pode executar vários comandos de CLI do ONTAP para criar a função de cluster do ONTAP e atribuir Privileges mínimo.

Passos

1. No sistema de storage, crie uma função e atribua todas as permissões à função.

   ```
   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 esse usuário.

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

3. Desbloquear o utilizador.

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

Comandos de CLI do ONTAP para criar funções de cluster e atribuir permissões

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

> A partir do SnapCenter 5,0, os usuários de administradores de cluster só são compatíveis com APIs REST. Se você quiser criar funções usando um administrador que não seja de cluster, use o ZAPI.

- `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

"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`

Configure pools de aplicativos do IIS para habilitar permissões de leitura do ative Directory

Você pode configurar os Serviços de informações da Internet (IIS) no servidor Windows para criar uma conta de pool de aplicativos personalizada quando precisar ativar as permissões de leitura do ative Directory para o SnapCenter.

Passos

1. Abra o Gerenciador do IIS no servidor Windows em que 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, em seguida, clique em **…** para editar a identidade do conjunto de aplicações SnapCenter.
5. No campo conta personalizada, insira um nome de usuário de domínio ou conta de administrador de domínio com permissão de leitura do ative Directory.
6. Clique em OK.

   A conta personalizada substitui a conta ApplicationPoolIdentity incorporada para o pool de aplicativos do SnapCenter.

Configurar as definições do registo de auditoria

Os logs de auditoria são gerados para cada atividade do servidor SnapCenter. Por padrão, os logs de auditoria são protegidos no local instalado padrão *C: Arquivos de programas/NetApp/SnapCenter WebApp/audit*.

Os logs de auditoria são protegidos por meio da geração de resumos assinados digitalmente para cada evento de auditoria para protegê-lo da modificação não autorizada. Os resumos gerados são mantidos no arquivo de checksum de auditoria separado e em seguida são verificações periódicas de integridade para garantir a integridade do conteúdo.

Você deve ter feito login como a função "SnapCenterAdmin".

Sobre esta tarefa

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

  Unidades compartilhadas ou montadas em rede não são suportadas.

- Se o protocolo UDP for usado nas configurações do servidor Syslog, os erros devido à porta estão inativos ou não podem 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 de cmdlet do software SnapCenter".

Passos

1. Na página **Configurações**, navegue até **Configurações** > **Configurações globais** > **Configurações do log de auditoria**.
2. Na secção Registo de auditoria, introduza os detalhes.
3. Digite o diretório **Audit log** e o diretório de log de checksum* de auditoria
   a. Introduza o tamanho máximo do ficheiro
   b. Introduza o máximo de ficheiros de registo

c. Insira a porcentagem de uso do espaço em disco para enviar um alerta

4. (Opcional) Ativar **Log UTC Time**.
5. (Opcional) ative **Audit Log Integrity Check Schedule** e clique em **Start Integrity Check** para verificação de integridade sob demanda.

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

6. (Opcional) ative os 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 o protocolo 'Trusted Root' para TLS 1,2.

   a. Introduza o sistema anfitrião do servidor Syslog
   b. Introduza a porta do servidor Syslog
   c. Introduza o protocolo Syslog Server
   d. Introduza o formato RFC

7. Clique em **Salvar**.
8. Você pode ver verificações de integridade de auditoria e verificações de espaço em disco clicando em **Monitor** > **jobs**.

Adicione sistemas de storage

Você deve configurar o sistema de armazenamento que dá acesso à SnapCenter ao armazenamento ONTAP ou ao Amazon FSX for NetApp ONTAP para executar operações de proteção de dados e provisionamento.

Você pode adicionar um SVM independente ou um cluster composto de vários SVMs. Se você estiver usando o Amazon FSX para NetApp ONTAP, você pode adicionar o FSX admin LIF composto por várias SVMs usando a conta fsxadmin ou adicionar o FSX SVM no SnapCenter.

Antes de começar

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

  As instalações de plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento, pois 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 do sistema de armazenamento devem ser exclusivos.

  O SnapCenter não é compatível com vários sistemas de storage com o mesmo nome em clusters diferentes. Cada sistema de storage com suporte do SnapCenter deve ter um nome exclusivo e um endereço IP de LIF de dados exclusivo.

Sobre esta tarefa

- Ao configurar sistemas de armazenamento, também pode ativar as funcionalidades do sistema de Gestão de Eventos (EMS) e do AutoSupport. A ferramenta AutoSupport coleta dados sobre a integridade do seu sistema e envia automaticamente os dados para o suporte técnico da NetApp, permitindo que eles solucionem o problema do seu sistema.

  Se você habilitar esses recursos, o SnapCenter enviará informações do AutoSupport para o sistema de armazenamento e mensagens do EMS para o syslog do sistema de armazenamento quando um recurso estiver protegido, uma operação de restauração ou clone terminar com êxito ou uma operação falhar.

- Se você está planejando replicar snapshots para um destino da SnapMirror ou destino da SnapVault, configure as conexões do sistema de storage para o SVM ou cluster de destino, bem como para o SVM ou cluster de origem.

Se alterar a palavra-passe do sistema de armazenamento, os trabalhos agendados, as operações de cópia de segurança a pedido e restauro poderão falhar. Depois de alterar a palavra-passe do sistema de armazenamento, pode atualizar a palavra-passe clicando em **Modificar** no separador armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Storage Systems**.
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 storage	Introduza o nome do sistema de armazenamento ou o endereço IP. Os nomes de sistemas de storage, que não incluem o nome de domínio, devem ter 15 ou menos carateres e os nomes devem ser solucionáveis. Para criar conexões do sistema de armazenamento com nomes com mais de 15 carateres, você pode usar o cmdlet Add-SmStorageConnectionPowerShell. Para sistemas de storage com configuração MetroCluster (MCC), recomenda-se Registrar clusters locais e de pares para operações sem interrupções. O SnapCenter não é compatível com vários SVMs com o mesmo nome em clusters diferentes. Cada SVM que seja compatível com o SnapCenter precisa ter um nome exclusivo. Depois de adicionar a conexão de storage 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, então ele precisa ser resolvido a partir do SnapCenter e do host do plug-in.
Nome de utilizador/Palavra-passe	Insira as credenciais do usuário de storage que tem o Privileges necessário para acessar o sistema de storage.

Para este campo…	Faça isso…
Sistema de Gestão de Eventos (EMS) e Definições do AutoSupport	Se você quiser enviar mensagens EMS para o syslog do sistema de armazenamento ou se quiser enviar mensagens AutoSupport para o 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 AutoSupport para operações com falha no sistema de armazenamento**, a caixa de seleção **Log SnapCenter eventos para syslog** também está selecionada porque mensagens EMS são necessárias para habilitar notificações 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 storage secundário em um relacionamento de backup, marque a caixa de seleção **secundário**. Quando a opção **secundário** está selecionada, o SnapCenter não executa uma verificação de licença imediatamente.

   Se você tiver adicionado SVM no SnapCenter, o usuário precisará selecionar o tipo de plataforma no menu suspenso manualmente.

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

      A porta padrão 443 normalmente funciona.

   c. Introduza o tempo em segundos que deve decorrer antes de as tentativas de comunicação serem interrompidas.

      O valor padrão é de 60 segundos.

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

Resultado

Na página sistemas de armazenamento, na lista suspensa **Type**, execute uma das seguintes ações:

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

  Se você adicionou FSX SVMs, os FSX SVMs são listados aqui.

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

  Se você adicionou clusters FSX usando fsxadmin, os clusters FSX são listados aqui.

  Quando você clica no nome do cluster, todos os SVMs que fazem parte do cluster são exibidos na seção máquinas virtuais de armazenamento.

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

Se você atualizou os sistemas de storage FAS ou AFF para todos os Arrays SAN (ASA), atualize a conexão de storage no servidor SnapCenter para refletir o novo tipo de storage no SnapCenter.

Depois de terminar

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

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

O administrador da máquina virtual de storage (SVM) não tem acesso ao AutoSupport.

Adicione licenças padrão baseadas em controladora SnapCenter

É necessária uma licença baseada em controlador padrão da SnapCenter se você estiver usando controladores de storage FAS, AFF ou All SAN Array (ASA).

A licença baseada no controlador tem as seguintes caraterísticas:

- Direito padrão da SnapCenter incluído na compra de pacote Premium ou Flash (não com o pacote básico)
- Uso ilimitado de armazenamento
- Habilitado adicionando-o diretamente ao controlador de storage FAS, AFF ou ASA usando a linha de comando Gerenciador de sistema do ONTAP ou cluster de storage

  Você não insere nenhuma informação de licença na GUI do SnapCenter para as licenças baseadas no controlador do SnapCenter.

- Bloqueado no número de série do controlador

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

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

Você pode usar a GUI do SnapCenter para ver se uma licença do SnapManager Suite está instalada em sistemas de storage primário FAS, AFF ou ASA e identificar quais sistemas de storage podem exigir licenças do SnapManager Suite. As licenças do SnapManager Suite se aplicam somente a SVMs ou clusters do FAS,

AFF e ASA em sistemas de storage primário.

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

Passos

1. No painel de navegação esquerdo, selecione **Storage Systems**.
2. Na página sistemas de armazenamento, na lista suspensa **tipo**, selecione se deseja exibir todos os SVMs ou clusters que foram adicionados:
   - Para visualizar todos os SVMs que foram adicionados, selecione **SVMs ONTAP**.
   - Para visualizar todos os clusters que foram adicionados, selecione **clusters ONTAP**.

     Quando você seleciona o nome do cluster, todos os SVMs que fazem parte do cluster são exibidos 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 storage primário FAS, AFF ou ASA.
   - Indica que uma licença do SnapManager Suite não está instalada em um sistema de storage 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 para NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select ou plataformas de armazenamento secundário.

Passo 2: Identifique 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.

> A licença baseada em controladora padrão do SnapCenter é exibida como licença SnapManagerSuite no controlador.

Passos

1. Faça login no controlador NetApp usando a linha de comando ONTAP.
2. Digite o comando license show e, em seguida, exiba a saída para determinar se a licença 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 é instalada, portanto, nenhuma ação adicional de licenciamento SnapCenter é necessária.

Passo 3: Recupere o número de série do controlador

Você precisa ter o número de série do controlador para recuperar o número de série da sua licença baseada no controlador. Você pode recuperar 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.

Passos

1. Faça login no controlador usando a linha de comando ONTAP.
2. Digite o comando system show -instance e, em seguida, 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. Registe os números de série.

Passo 4: Recupere o número de série da licença baseada no controlador

Se você estiver usando o armazenamento FAS ou AFF, poderá recuperar a licença baseada no controlador SnapCenter do site de suporte da NetApp antes de instalá-la 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, nenhuma informação será retornada para sua pesquisa.

- Você deve ter o número de série do controlador.

Passos

1. Inicie sessão 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) está selecionado, introduza o número de série do controlador e, em seguida, selecione **Go!**.

É apresentada uma lista de licenças para o controlador especificado.

4. Localize e Registre a licença padrão ou SnapManagerSuite do SnapCenter.

Passo 5: Adicione licença baseada no controlador

Você pode usar a linha de comando ONTAP para adicionar uma licença baseada em controladora SnapCenter quando estiver usando sistemas FAS, AFF ou ASA e tiver uma licença padrão ou SnapManagerSuite do SnapCenter.

Antes de começar

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

Sobre esta tarefa

Se você quiser instalar o SnapCenter de avaliação com o storage FAS, AFF ou ASA, obtenha uma licença de avaliação do pacote Premium para instalar no controlador.

Se você quiser instalar o SnapCenter em uma base de avaliação, entre em Contato com seu representante de vendas para obter uma licença de avaliação do pacote Premium para instalar em seu controlador.

Passos

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

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

   Este comando está disponível no nível de privilégios de administrador.

3. Verifique se a licença SnapManagerSuite está instalada:

```
license show
```

Passo 6: Remova a licença de teste

Se você estiver usando uma licença padrão SnapCenter baseada em controlador e precisar remover a licença de avaliação baseada em capacidade (número de série que termina com "'50""), você deve usar os comandos MySQL para remover a licença de teste manualmente. A licença de teste não pode ser excluída usando a GUI do SnapCenter.

> A remoção manual de uma licença de teste só é necessária se estiver a utilizar uma licença baseada em controlador padrão da SnapCenter.

Passos

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

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

   O MySQL solicita a senha. Introduza as credenciais fornecidas durante a reposição da palavra-passe.
3. Remova a licença de teste do banco de dados:

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

Provisione seu sistema de storage

Provisione storage em hosts do Windows

Configurar armazenamento LUN

Pode utilizar o SnapCenter para configurar um LUN ligado a FC ou ligado a iSCSI. Você também pode usar o SnapCenter para conetar um LUN existente a um host do Windows.

LUNs são a unidade básica de armazenamento em uma configuração SAN. O host do Windows vê LUNs no seu sistema como discos virtuais. Para obter mais informações, "Guia de configuração de SAN ONTAP 9"consulte .

Estabeleça uma sessão iSCSI

Se estiver a utilizar iSCSI para ligar a um LUN, tem de estabelecer uma sessão iSCSI antes de criar o LUN para ativar a comunicação.

Antes de começar

- Você deve ter definido o nó do sistema de storage como um destino iSCSI.

- Tem de ter iniciado o serviço iSCSI no sistema de armazenamento. "Saiba mais"

Sobre esta tarefa

Pode estabelecer uma sessão iSCSI apenas entre as mesmas versões IP, de IPv6 a IPv6, ou de IPv4 a IPv4.

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

Se alterar o nome de um iniciador iSCSI, o acesso a iSCSI Targets é afetado. Depois de alterar o nome, você pode precisar reconfigurar os destinos acessados pelo iniciador para que eles possam reconhecer o novo nome. Tem de se certificar de que reinicia o anfitrião depois de alterar o nome de um iniciador iSCSI.

Se o seu host tiver mais de uma interface iSCSI, depois de estabelecer uma sessão iSCSI para SnapCenter usando um endereço IP na primeira interface, não será possível 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 **iSCSI Session**.
3. Na lista suspensa **Storage Virtual Machine**, selecione a máquina virtual de armazenamento (SVM) para o destino iSCSI.
4. Na lista suspensa **Host**, selecione o host para a sessão.
5. Clique em **estabelecer sessão**.

   É apresentado o assistente estabelecer sessão.

6. No assistente estabelecer sessão, identifique o alvo:

Neste campo…	Digite…
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 no formato somente leitura.
Endereço do portal de destino	O endereço IP do portal de rede de destino
Porta do portal de destino	A porta TCP do portal de rede de destino
Endereço do portal do iniciador	O endereço IP do portal de rede do iniciador

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

   O SnapCenter estabelece a sessão iSCSI.

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

Desligar uma sessão iSCSI

Ocasionalmente, pode ser necessário desconetar uma sessão iSCSI de um destino com o qual você tem várias sessões.

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **iSCSI Session**.
3. Na lista suspensa **Storage Virtual Machine**, selecione a máquina virtual de armazenamento (SVM) para o destino iSCSI.
4. Na lista suspensa **Host**, selecione o host para a sessão.
5. Na lista de sessões iSCSI, selecione a sessão que deseja desconetar e clique em **desconetar sessão**.
6. Na caixa de diálogo desconetar sessão, clique em **OK**.

   O SnapCenter desliga a sessão iSCSI.

Crie e gerencie grupos

Você cria grupos de iniciadores (grupos de iniciadores) 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 grupo em um host do Windows.

Crie um grupo

Você pode usar o SnapCenter para criar um grupo em um host do Windows. O grupo estará disponível no assistente criar disco ou conetar disco quando você mapear o grupo 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 grupo, defina o grupo:

Neste campo…	Faça isso…
Sistema de storage	Selecione o SVM para o LUN que você mapeará para o grupo.
Host	Selecione o host no qual você deseja criar o grupo.
Nome do grupo	Introduza o nome do grupo.
Iniciadores	Selecione o iniciador.

Neste campo…	Faça isso…
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 grupo no sistema de armazenamento.

Renomeie um grupo

Você pode usar o SnapCenter para renomear um grupo 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 **Storage Virtual Machine** para exibir uma lista de SVMs disponíveis e selecione o SVM para o grupo que deseja renomear.
4. Na lista de grupos para o SVM, selecione o grupo que deseja renomear e clique em **Renomear**.
5. Na caixa de diálogo Renomear grupo, digite o novo nome para o grupo e clique em **Renomear**.

Modifique um grupo

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

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 **Storage Virtual Machine** para exibir uma lista suspensa de SVMs disponíveis e, em seguida, selecione o SVM para o grupo que deseja modificar.
4. Na lista de grupos, selecione um grupo e clique em **Adicionar iniciador ao grupo**.
5. Selecione um host.
6. Selecione os iniciadores e clique em **OK**.

Exclua um igroup

Você pode usar o SnapCenter para excluir um iggroup 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 **Storage Virtual Machine** para exibir uma lista suspensa de SVMs disponíveis e, em seguida, selecione o SVM para o grupo que deseja excluir.

4. Na lista de grupos para o SVM, selecione o grupo que deseja excluir e clique em **Excluir**.
5. Na caixa de diálogo Excluir grupo, clique em **OK**.

   O SnapCenter exclui o grupo.

Criar e gerenciar discos

O host do Windows vê LUNs no seu sistema de armazenamento como discos virtuais. Pode utilizar o SnapCenter para criar e configurar um LUN ligado a FC ou ligado a iSCSI.

- O SnapCenter suporta apenas discos básicos. Os discos dinâmicos não são suportados.
- Para GPT apenas é permitida uma partição de dados e para MBR uma partição primária que tenha um volume formatado com NTFS ou CSVFS e tenha um caminho de montagem.
- Estilos de partição suportados: GPT, MBR; em uma VM UEFI VMware, 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.

Exibir os discos em um host

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

Passos

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

   Os discos são listados.

Exibir discos em cluster

É possível exibir discos em cluster no cluster que você gerencia com o SnapCenter. Os discos em cluster são exibidos somente quando você seleciona o cluster na lista suspensa hosts.

Passos

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

   Os discos são listados.

Crie LUNs ou discos conectados a FC ou iSCSI

O host do Windows vê os LUNs no seu sistema de armazenamento como discos virtuais. Pode utilizar o SnapCenter para criar e configurar um LUN ligado a FC ou ligado a iSCSI.

Se você quiser criar e formatar discos fora do SnapCenter, apenas os sistemas de arquivos NTFS e CSVFS

são suportados.

Antes de começar

- Você deve ter criado um volume para o LUN em seu sistema de storage.

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

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

- Você deve ter iniciado o serviço FC ou iSCSI no sistema de storage.
- Se estiver a utilizar iSCSI, tem de 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 conetar 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 cluster.

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **Disks**.
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 storage	Selecione o SVM para o LUN.
Caminho de LUN	Clique em **Browse** para selecionar o caminho completo da pasta que contém o LUN.
Nome da LUN	Introduza o nome do LUN.
Tamanho do cluster	Selecione o tamanho da alocação do bloco LUN para o cluster. O tamanho do cluster depende do sistema operacional e dos aplicativos.
Etiqueta LUN	Opcionalmente, insira 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. Digite 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 de cluster (CSV)	O LUN é compartilhado por hosts em um cluster de failover do Windows Server que usa CSV. Digite 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 é o proprietário do grupo de cluster.

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

Propriedade	Descrição
Atribuir automaticamente o 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 cria um ponto de montagem de volume sob a unidade C: (C:). A atribuição automática não é suportada para discos partilhados.
Atribua a letra da unidade	Monte o disco na unidade selecionada na lista suspensa adjacente.
Utilize o ponto de montagem do volume	Monte o disco no caminho da unidade especificado no campo adjacente. A raiz do ponto de montagem de volume deve ser propriedade do host no qual você está criando o disco.
Não atribua a letra da unidade ou o ponto de montagem do volume	Escolha esta opção se preferir montar o disco manualmente no Windows.

Propriedade	Descrição
Tamanho da LUN	Especifique o tamanho do LUN; mínimo de 150 MB. Selecione MB, GB ou TB na lista suspensa adjacente.
Use thin Provisioning para o volume que hospeda este LUN	Thin Provisioning o LUN. O thin Provisioning aloca apenas o espaço de armazenamento necessário de uma só vez, permitindo que o LUN cresça eficientemente até à capacidade máxima disponível. Certifique-se de que há espaço suficiente disponível no volume para acomodar todo o armazenamento LUN que você acha que vai precisar.
Escolha o tipo de partição	Selecione partição GPT para uma Tabela de partição GUID ou partição MBR para um Registro de inicialização mestre. As partições MBR podem causar problemas de desalinhamento nos clusters de failover do Windows Server. Os discos de partição UEFI (Unified Extensible firmware Interface) não são suportados.

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

Neste campo…	Faça isso…
Host	Clique duas vezes no nome do grupo de cluster para exibir uma lista suspensa que mostra os hosts que pertencem ao cluster e, em seguida, selecione o host para o iniciador. Este campo é 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 multipath (MPIO).

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

grupo:

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

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

    O SnapCenter cria o LUN e o coneta à unidade especificada ou ao caminho da unidade no host.

Redimensione um disco

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

Sobre esta tarefa

- Para LUN com provisionamento reduzido, o tamanho da geometria do lun ONTAP é mostrado como o tamanho máximo.
- Para LUN provisionado grosso, o tamanho expansível (tamanho disponível no volume) é mostrado como o tamanho máximo.
- Os LUNs com partições de estilo MBR têm um limite de tamanho de 2 TB.
- Os LUNs com partições de estilo GPT têm um limite de tamanho de sistema de armazenamento de 16 TB.
- É uma boa ideia fazer um instantâneo antes de redimensionar um LUN.
- Se você precisar restaurar um LUN de uma captura Instantânea feita antes que o LUN fosse redimensionado, o SnapCenter redimensionará automaticamente o LUN para o tamanho da captura Instantânea.

  Após a operação de restauração, os dados adicionados ao LUN após o dimensionamento devem ser restaurados a partir de uma captura Instantânea feita após o dimensionamento.

Passos

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

   Os discos são 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, será necessário clicar fora do campo tamanho antes que o botão diminuir ou expandir esteja 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 **Shrink** ou **Expand**, conforme apropriado.

   O SnapCenter redimensiona o disco.

Conete um disco

Você pode usar o assistente conetar disco para conetar um LUN existente a um host ou para reconetar um LUN que foi desconetado.

Antes de começar

- Você deve ter iniciado o serviço FC ou iSCSI no sistema de storage.
- Se estiver a utilizar iSCSI, tem de ter estabelecido uma sessão iSCSI com o sistema de armazenamento.
- Não é possível conetar 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), será necessário conetar o disco no host que possui o grupo de cluster.
- O plug-in para Windows precisa ser instalado apenas no host no qual você está conetando o disco.

Passos

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

   O assistente Connect Disk (ligar disco) é aberto.

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

Neste campo…	Faça isso…
Sistema de storage	Selecione o SVM para o LUN.
Caminho de LUN	Clique em **Procurar** para selecionar o caminho completo do volume que contém o LUN.
Nome da LUN	Introduza o nome do LUN.

Neste campo…	Faça isso…
Tamanho do cluster	Selecione o tamanho da alocação do bloco LUN para o cluster. O tamanho do cluster depende do sistema operacional e dos aplicativos.
Etiqueta LUN	Opcionalmente, insira 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 conetar o disco a um host no cluster de failover.
Volume compartilhado de 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 conetando ao disco é o proprietário do grupo de cluster.

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

Propriedade	Descrição
Atribuição automática	Permita que o SnapCenter atribua 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 cria um ponto de montagem de volume sob a unidade C: (C:). A propriedade atribuição automática não é suportada para discos compartilhados.
Atribua a letra da unidade	Monte o disco na unidade selecionada na lista suspensa adjacente.

Propriedade	Descrição
Utilize o ponto de montagem do volume	Monte o disco no caminho da unidade especificado no campo adjacente. A raiz do ponto de montagem de volume deve ser propriedade do host no qual você está criando o disco.
Não atribua a letra da unidade ou o ponto de montagem do volume	Escolha esta opção se preferir montar o disco manualmente no Windows.

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

Neste campo…	Faça isso…
Host	Clique duas vezes no nome do grupo de cluster para exibir uma lista suspensa que mostra os hosts que pertencem ao cluster e, em seguida, selecione o host para o iniciador. Este campo é 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 grupo existente para o LUN ou criar um novo grupo:

Selecione…	Se…
Crie um novo grupo para iniciadores selecionados	Você deseja criar um novo grupo para os iniciadores selecionados.
Escolha um grupo existente ou especifique um novo grupo para iniciadores selecionados	Você deseja especificar um grupo existente para os iniciadores selecionados ou criar um novo grupo com o nome que você especificar. Digite o nome do grupo no campo **Nome do grupo**. Digite as primeiras letras do nome do grupo existente para completar automaticamente o campo.

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

    O SnapCenter coneta o LUN à unidade especificada ou ao caminho da unidade no host.

Desconete um disco

Você pode desconetar um LUN de um host sem afetar o conteúdo do LUN, com uma exceção: Se você desconetar um clone antes que ele tenha sido dividido, você perderá o conteúdo do clone.

Antes de começar

- Certifique-se de que o LUN não está a ser utilizado por qualquer aplicação.
- Certifique-se de que o LUN não está a ser monitorizado com o software de monitorização.
- Se o LUN for compartilhado, remova as dependências de recursos do cluster do LUN e verifique se todos os nós do cluster estão ligados, funcionando corretamente e disponíveis para o SnapCenter.

Sobre esta tarefa

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

Para evitar a eliminação automática do volume FlexClone, deve mudar o nome do volume antes de desligar o último LUN. Ao renomear o volume, certifique-se de alterar vários carateres do que apenas o último caractere no nome.

Passos

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

   Os discos são listados.

4. Selecione o disco que deseja desconetar e clique em **Disconnect**.
5. Na caixa de diálogo Disconnect Disk (Desligar disco), clique em **OK**.

   O SnapCenter desliga o disco.

Eliminar um disco

Você pode excluir um disco quando não precisar mais dele. Depois de eliminar um disco, não pode anular a sua eliminação.

Passos

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

   Os discos são 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.

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

Os modelos encapsulam as práticas recomendadas 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 fazendo isso, você pode criar seus próprios modelos seguindo os modelos fornecidos. Você deve revisar os parâmetros na documentação do cmdlet antes de criar um modelo personalizado.

Crie um compartilhamento SMB

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

Não é possível usar o SnapCenter para fazer backup de bancos de dados em compartilhamentos SMB. O suporte a SMB está limitado apenas ao provisionamento.

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **shares**.
3. Selecione o SVM na lista suspensa **Storage Virtual Machine**.
4. Clique em **novo**.

   Abre-se a caixa de diálogo New Share (Nova partilha).

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

Neste campo…	Faça isso…
Descrição	Introduza texto descritivo para a partilha.

Neste campo…	Faça isso…
Nome da partilha	Introduza o nome da partilha, por exemplo, test_share. O nome introduzido para a partilha também será utilizado como o nome do volume. O nome da partilha: • Deve ser uma string UTF-8. • Não deve incluir os seguintes carateres: Controlar carateres de 0x00 a 0x1F (ambos incluídos), 0X22 (aspas duplas) e os carateres especiais `\ / [ ] : (vertical bar) < > + = ; , ?`
Compartilhar caminho	• Clique no campo para introduzir um novo caminho do sistema de ficheiros, por exemplo, /. • Clique duas vezes no campo para selecionar a partir de 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 na 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 **shares**.
3. Na página compartilhamentos, clique no campo **Storage Virtual Machine** para exibir uma lista suspensa com uma lista de máquinas virtuais de armazenamento disponíveis (SVMs) e selecione o SVM para o compartilhamento que 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 storage

Embora o NTFS rastreie o espaço disponível em um LUN quando os arquivos são excluídos ou modificados, ele não relata as novas informações para o sistema de

armazenamento. Você pode executar o cmdlet PowerShell de recuperação de espaço no host Plug-in para Windows para garantir que os blocos recém-liberados sejam marcados como disponíveis no storage.

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

Antes de começar

- Você deve garantir que o processo de recuperação de espaço foi 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 cluster.
- Para um desempenho de armazenamento ideal, você deve executar a recuperação de espaço o mais frequentemente possível.

  Você deve garantir que todo o sistema de arquivos NTFS foi digitalizado.

Sobre esta tarefa

- A recuperação de espaço é demorada e intensiva na CPU, por isso geralmente é melhor executar a operação quando o sistema de armazenamento e o uso de host do Windows são baixos.
- A recuperação de espaço recupera quase todo o espaço disponível, mas não 100%.
- Você não deve executar a desfragmentação do disco ao mesmo tempo que está executando a recuperação de espaço.

  Fazer isso pode retardar o processo de recuperação.

Passo

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.

Provisione o armazenamento usando cmdlets do PowerShell

Se você 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 fornecidos pelo plug-in do SnapCenter para Microsoft Windows. Você pode usar cmdlets diretamente ou adicioná-los a scripts.

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

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

Se os cmdlets do SnapCenter PowerShell estiverem quebrados devido à remoção do SnapDrive para Windows do servidor, "Cmdlets SnapCenter quebrados quando o SnapDrive for Windows é desinstalado"

consulte .

Provisione storage em ambientes VMware

Você pode usar o plug-in do SnapCenter para Microsoft Windows em ambientes VMware para criar e gerenciar LUNs e snapshots.

Plataformas VMware Guest os compatíveis

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

  Suporte para até um máximo de 16 nós com suporte no VMware ao usar o iniciador de software iSCSI da Microsoft ou até dois nós usando FC

- LUNs RDM

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

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

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

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.
- Quando você cria um LUN RDM fora do plug-in para Windows, você deve reiniciar o serviço de plug-in para permitir que ele reconheça o disco recém-criado.
- Não é possível usar iniciadores iSCSI e FC ao mesmo tempo em um SO convidado VMware.

Mínimo do vCenter Privileges necessário para operações do SnapCenter RDM

Você deve ter o seguinte vCenter Privileges no host para executar operações RDM em um SO convidado:

- Datastore: Remover Arquivo
- Host: Configuração > Configuração da partição de armazenamento
- Máquina virtual: Configuração

Você deve atribuir esses Privileges a uma função no nível do servidor do Centro Virtual. A função à qual você atribui esses Privileges não pode ser atribuída a nenhum usuário sem root Privileges.

Depois de atribuir esses Privileges, você pode instalar o plug-in para Windows no SO convidado.

Gerenciar LUNs FC RDM em um cluster da Microsoft

Você pode usar o Plug-in para Windows para gerenciar um cluster da Microsoft usando LUNs FC RDM, mas primeiro você deve criar o quórum 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 o 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 oferece suporte a 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 de 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 datastore 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 uma SAN FC.

  Se necessário, o armazenamento de dados compartilhado também pode ser criado por 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.

  Não é possível 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 requer que você configure o controlador SCSI SAS LSI Logic em cada máquina virtual. Os LUNs compartilhados não podem usar o controlador SAS LSI Logic existente se apenas um de seu tipo existir e já estiver conetado à unidade C:.

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

  > Quando você adiciona 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 **Create a new disk** no VMware Infrastructure Client.

- Os clusters de máquinas virtuais da Microsoft não podem fazer parte de um cluster VMware.
- Você deve usar as credenciais do vCenter e não as credenciais do ESX ou do 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 grupo com iniciadores de vários hosts.

  O grupo que contém 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 LUN RDM no ESXi 5,0 usando um iniciador FC.

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

Limitações

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

Esse recurso não é suportado em versões anteriores ao ESX 5,5i.

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

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

- Iniciadores iSCSI ESX e HBAs não são suportados em discos compartilhados em um cluster Microsoft.
- O Plug-in para Windows não suporta migração de máquina virtual com o vMotion se a máquina virtual fizer parte de um cluster da Microsoft.
- O plug-in para Windows não suporta MPIO em máquinas virtuais em um cluster da Microsoft.

Crie um LUN FC RDM compartilhado

Antes de usar LUNs FC RDM para compartilhar o storage entre nós em um cluster da Microsoft, primeiro você deve criar o disco de quorum compartilhado e o disco de storage compartilhado e adicioná-los a ambas as 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, "Cluster de máquinas virtuais em hosts físicos"consulte .

Configure conexões MySQL seguras com o servidor SnapCenter

Você pode gerar certificados SSL (Secure Sockets Layer) e arquivos de chave se quiser proteger a comunicação entre o servidor SnapCenter e o servidor MySQL em configurações autônomas ou configurações NLB (Network Load Balancing).

Configurar conexões MySQL seguras para configurações autônomas do servidor SnapCenter

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

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 arquivos de chave para servidores e clientes MySQL no Windows usando o comando openssl.

   Para obter informações, consulte "MySQL versão 5,7: Criando certificados SSL e chaves usando openssl"

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

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

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

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

3. Atualize o certificado CA, o certificado público do servidor, o certificado público do cliente, a chave privada do servidor e os caminhos de chave privada do cliente no ficheiro 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 o certificado CA, o certificado público do servidor e os caminhos de chave privada do servidor na seção [mysqld] do arquivo de configuração do servidor MySQL (my.ini).

   Você deve especificar o certificado CA, o certificado público do cliente e os caminhos de 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 [cliente] 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 da Web do servidor SnapCenter no servidor de informações da Internet (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 [cliente] do arquivo my.ini.

   O exemplo a seguir mostra os caminhos atualizados na seção [cliente] 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 da Web do servidor SnapCenter no IIS.

Configurar conexões MySQL seguras para configurações HA

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

Os seguintes certificados são gerados:

- Certificado CA

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

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

Passos

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

   Para obter informações, consulte "MySQL versão 5,7: Criando certificados SSL e chaves usando openssl"

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

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

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

   O caminho padrão da pasta de dados MySQL é C:/// NetApp/ SnapCenter/ dados MySQL.

3. Atualize o certificado CA, o certificado público do servidor, o certificado público do cliente, a chave privada do servidor e os caminhos de chave privada do cliente no ficheiro 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 o certificado CA, o certificado público do servidor e os caminhos de chave privada do servidor na seção [mysqld] do arquivo de configuração do servidor MySQL (my.ini).

   Você deve especificar o certificado CA, o certificado público do cliente e os caminhos de 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 dados/dados.

   ```
   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 [cliente] 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 da 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.

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

      O caminho padrão da pasta de dados MySQL é C:/// NetApp/ SnapCenter/ dados MySQL.

      > 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 arquivos de chave para servidores MySQL e clientes no Windows usando o comando openssl.

      "MySQL versão 5,7: Criando certificados SSL e chaves usando openssl"

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

      Recomenda-se usar o FQDN do servidor como o nome comum para o certificado do servidor.

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

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

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

Você deve especificar o certificado CA, o certificado público do cliente e os caminhos de 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 dados/dados.

```
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 [cliente] 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 da Web do servidor SnapCenter no servidor de informações da Internet (IIS) em ambos os nós de HA.
6. Reinicie o serviço MySQL em ambos os nós de HA.
7. Atualize o valor da chave MySQLProtocol no arquivo SnapManager.Web.UI.dll.config para ambos os nós de 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 especificados na seção [cliente] do arquivo my.ini para ambos os nós de HA.

O exemplo a seguir mostra os caminhos atualizados na seção [cliente] 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 da Web do servidor SnapCenter no IIS em ambos os nós de HA.
10. Use o cmdlet Set-SmRepositoryConfig -RebuildSlave -Force PowerShell com a opção -Force em um dos nós de HA para estabelecer replicação MySQL segura em ambos os nós de HA.

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

Recursos ativados em seu host Windows durante a instalação

O instalador do servidor SnapCenter permite os recursos e funções do Windows em seu host Windows durante a instalação. Isso pode ser de interesse para fins de solução de problemas e manutenção do sistema host.

Categoria	Recurso
Servidor Web	• Serviços de informações da Internet • Serviços Web mundiais • Recursos HTTP comuns ◦ Documento padrão ◦ Navegação de diretório ◦ Erros HTTP ◦ Redirecionamento HTTP ◦ Conteúdo estático ◦ Publicação WebDAV • Saúde e Diagnóstico ◦ Registo personalizado ◦ Registo HTTP ◦ Ferramentas de registo ◦ Monitorização de pedidos ◦ Traçado • Recursos de desempenho ◦ Compressão de conteúdo estático • Segurança ◦ Segurança IP ◦ Autenticação básica ◦ Suporte centralizado a certificados SSL ◦ Autenticação Mapeamento certificado Cliente ◦ Autenticação de mapeamento de certificados do cliente IIS ◦ Restrições de IP e domínio ◦ Filtragem de solicitação ◦ Autorização de URL ◦ Autenticação do Windows • Recursos de desenvolvimento de aplicativos ◦ Extensão .NET 4,5 ◦ Inicialização da aplicação ◦ Pacote de Hospedagem ASP.NET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes ◦ O lado do servidor inclui ◦ Protocolo WebSocket • Ferramentas de gerenciamento Console de gerenciamento do IIS

Categoria	Recurso
Scripts e ferramentas de gerenciamento do IIS	• Serviço de Gestão do IIS • Ferramentas de gerenciamento da Web
O NET Framework 8.0.5 é um dos nossos selecionados Jogos de Plataforma	• .NET Framework começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • ASP.NET começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • Windows Communication Foundation (WCF) HTTP Activation45 ◦ Ativação TCP ◦ Ativação HTTP Para obter informações específicas de solução de problemas .NET, "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet" consulte .
Serviço de ativação do processo do Windows	Modelo do processo
APIs de configuração	Tudo

Recursos ativados no host Linux durante a instalação

O servidor SnapCenter instala os pacotes de software abaixo, estes podem ser de interesse para fins de solução de problemas e manutenção do sistema host.

- Rabbitmq
- Nginx
- Erlang
- .NET Framework começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes
- PAM-devel
- PowerShell

Proteja bancos de dados Microsoft SQL Server

Plug-in do SnapCenter para Microsoft SQL Server

Visão geral do plug-in do SnapCenter para Microsoft SQL Server

O plug-in do SnapCenter para Microsoft SQL Server é um componente do lado do host do software NetApp SnapCenter que permite o gerenciamento de proteção de dados com reconhecimento de aplicativos de bancos de dados do Microsoft SQL Server. O plug-in para SQL Server automatiza as operações de backup, verificação, restauração e clone de banco de dados do SQL Server em seu ambiente SnapCenter.

Quando o plug-in para SQL Server é instalado, você pode 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 replicação de backup de disco para disco para fins de conformidade ou arquivamento de padrões.

O que você pode fazer com o plug-in SnapCenter para Microsoft SQL Server

Quando o plug-in do SnapCenter for instalado no seu ambiente, você pode 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 clone 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 de sistema mestre e msdb. No entanto, você pode criar backups de log para o banco de dados do sistema modelo.

- Restaure os 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.
- Criar clones pontuais de bancos de dados de produção

  Não é possível executar operações de backup, restauração, clone e clone do ciclo de vida em bancos de dados do sistema tempdb.

- Verifique as operações de backup imediatamente ou adie a verificação até mais tarde

  A verificação do banco de dados do sistema do SQL Server não é suportada. O SnapCenter clones os bancos de dados para executar a operação de verificação. O SnapCenter não pode clonar bancos de dados do sistema do SQL Server e, portanto, a verificação desses bancos de dados não é suportada.

- Programe operações de backup e operações de clone
- Monitore operações de backup, operações de restauração e operações de clone

O Plug-in para SQL Server não suporta backup e recuperação de bancos de dados SQL Server em compartilhamentos SMB.

Plug-in do SnapCenter para recursos do Microsoft SQL Server

O plug-in para SQL Server é integrado ao Microsoft SQL Server no host do Windows e com a tecnologia NetApp Snapshot no sistema de storage. Para trabalhar com o plug-in para SQL Server, use a interface do SnapCenter.

O Plug-in para SQL Server inclui estes principais recursos:

- * Interface gráfica unificada do usuário com SnapCenter*

  A interface do SnapCenter fornece padronização e consistência entre plug-ins e ambientes. A interface do SnapCenter permite concluir processos consistentes de backup e restauração em plug-ins, usar relatórios centralizados, usar visualizações de dashboard rápidas, configurar controle de acesso baseado em funções (RBAC) e monitorar tarefas em todos os plug-ins. O SnapCenter também oferece gerenciamento centralizado de políticas e agendamento para dar suporte a operações de backup e clone.

- * Administração central automatizada*

  Você pode agendar backups de rotina do SQL Server, configurar a retenção de backup baseada em políticas e configurar operações de restauração pontuais e atualizadas. Você também pode monitorar proativamente seu ambiente SQL Server configurando o SnapCenter para enviar alertas de e-mail.

- **Tecnologia NetApp Snapshot sem interrupções**

  O plug-in para SQL Server usa a tecnologia Snapshot do NetApp com o plug-in NetApp SnapCenter para Microsoft Windows. Isso permite que você faça backup de bancos de dados em segundos e restaurá-los rapidamente sem deixar o SQL Server offline. Os snapshots consomem espaço mínimo de storage.

Além desses principais recursos, o Plug-in para SQL Server oferece os seguintes benefícios:

- Suporte ao fluxo de trabalho de backup, restauração, clone e verificação
- Delegação de funções centralizada e segurança compatível com RBAC
- Criação de cópias pontuais e com uso eficiente de espaço de bancos de dados de produção para teste ou extração de dados usando a tecnologia NetApp FlexClone

  É necessária uma licença FlexClone no sistema de storage que mantém o clone.

- Verificação de backup sem interrupções e automatizada
- Capacidade de executar vários backups ao mesmo tempo em vários servidores
- Cmdlets do PowerShell para scripts de operações de backup, verificação, restauração e clone
- Suporte para AlwaysOn Availability Groups (AGS) no SQL Server para acelerar as operações de configuração, backup e restauração AG
- Banco de dados in-memory e Buffer Pool Extension (BPE) como parte do SQL Server 2014
- Suporte para backup de LUNs e discos de máquina virtual (VMDKs)
- Suporte para infraestruturas físicas e virtualizadas
- Suporte para iSCSI, Fibre Channel, FCoE, mapeamento de dispositivos brutos (RDM) e VMDK em NFS e

VMFS

> Os volumes nas devem ter uma política de exportação padrão na máquina virtual de storage (SVM).

- Suporte para FileStream e grupo de arquivos em bancos de dados autônomos do SQL Server.
- Suporte para memória não volátil Express (NVMe) no Windows Server 2022
  - Workflows de backup, restauração, clone e verificação no layout VMDK criado no NVMe em TCP/IP.
  - Suporta a versão 1,3 do firmware NVMe a partir da atualização 2 do ESX 8,0 e requer a versão 21 do hardware virtual.
  - O WSFC (Cluster de failover do Windows Server) não é compatível com aplicativos em VMDK em NVMe em TCP/IP.
- É compatível com a sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), que permite que os serviços empresariais continuem operando mesmo em caso de falha completa do local, oferecendo suporte para failover transparente de aplicações usando uma cópia secundária. Nem a intervenção manual nem o script adicional são necessários para acionar um failover com a sincronização ativa do SnapMirror.

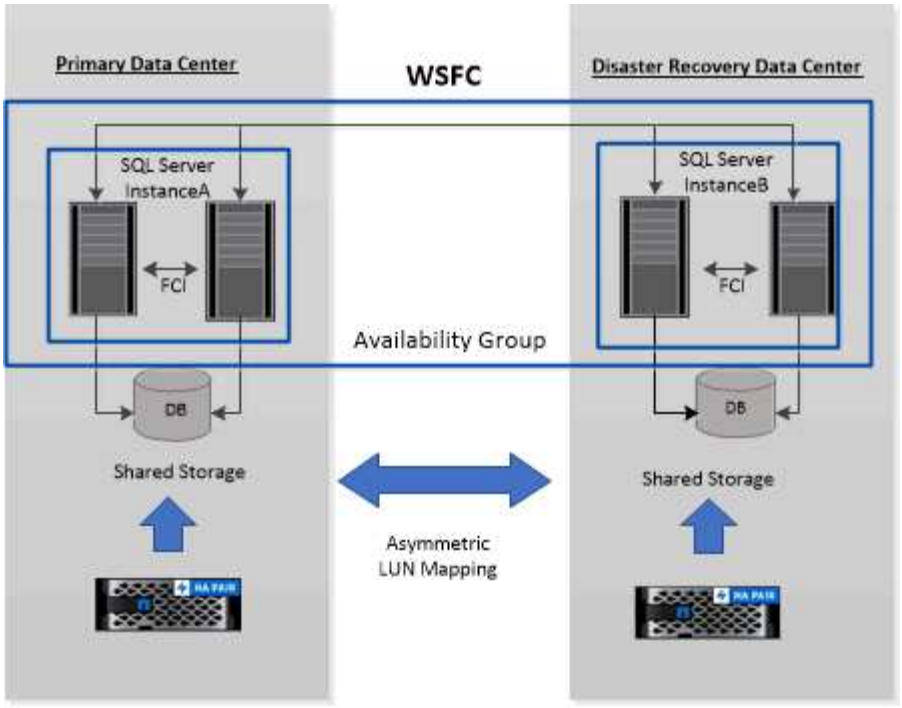
Suporte para mapeamento LUN assimétrico em clusters Windows

O plug-in do SnapCenter para Microsoft SQL Server suporta a descoberta no SQL Server 2012 e posterior, configurações de mapeamento 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 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.

Segue-se um exemplo de uma configuração ALM:

- Duas instâncias de cluster de failover (FCI) em um data center de vários locais
- FCI para alta disponibilidade local (HA) e Availability Group (AG) para recuperação de desastres com uma instância autônoma no local de recuperação de desastres



WSFC----Windows Server Failover Cluster

O storage no data center principal é compartilhado entre os nós de FCI presentes no data center principal. O storage no data center de recuperação de desastres é compartilhado entre os nós FCI presentes no data center de recuperação de desastres.

O storage no data center principal não é visível para os nós no data center de recuperação de desastres e vice-versa.

A arquitetura DO ALM combina duas soluções de storage compartilhado usadas pelo FCI, com uma solução de storage não compartilhada ou dedicada usada pelo SQL AG. A solução AG usa letras de unidade idênticas para recursos de disco compartilhados entre data centers. Esse arranjo de storage, em que um disco de cluster é compartilhado entre um subconjunto de nós dentro de um WSFC, é conhecido como ALM.

Tipos de storage compatíveis com o plug-in SnapCenter para Microsoft SQL Server

O SnapCenter suporta uma ampla variedade de tipos de armazenamento em máquinas físicas e máquinas virtuais. Você deve verificar se há suporte disponível para o seu tipo de armazenamento antes de instalar o pacote para o seu host.

O suporte para provisionamento e proteção de dados do SnapCenter está disponível no Windows Server. Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Máquina	Tipo de armazenamento	Provisione usando	Notas de suporte
Servidor físico	LUNs conectados a FC	Cmdlets da interface gráfica do usuário (GUI) do SnapCenter ou do PowerShell	

Máquina	Tipo de armazenamento	Provisione usando	Notas de suporte
Servidor físico	LUNs ligados ao iSCSI	Cmdlets SnapCenter GUI ou PowerShell	
Servidor físico	Compartilhamentos de SMB3 TB (CIFS) residentes em uma máquina virtual de storage (SVM)	Cmdlets SnapCenter GUI ou PowerShell	Suporte apenas para provisionamento.
VMware VM	LUNs RDM ligados por um FC ou iSCSI HBA	Cmdlets do PowerShell	
VMware VM	ISCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets SnapCenter GUI ou PowerShell	
VMware VM	Armazenamentos de dados NFS ou VMFS (Virtual Machine File Systems)	VMware vSphere	
VMware VM	Um sistema convidado conetado a SMB3 compartilhamentos residentes em um SVM	Cmdlets SnapCenter GUI ou PowerShell	Suporte apenas para provisionamento.
VMware VM	Armazenamentos de dados da VVol em NFS e SAN	Ferramentas do ONTAP para VMware vSphere	

Máquina	Tipo de armazenamento	Provisione usando	Notas de suporte
VM Hyper-V	LUNs de FC virtual (VFC) conectados por um switch Fibre Channel virtual	Cmdlets SnapCenter GUI ou PowerShell	Você deve usar o Hyper-V Manager para provisionar LUNs Virtual FC (VFC) conectados por um switch Fibre Channel virtual. O Hyper-V passa por discos e faz backup de bancos de dados em VHD(x) que são provisionados no armazenamento NetApp não são suportados.
VM Hyper-V	ISCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets SnapCenter GUI ou PowerShell	O Hyper-V passa por discos e faz backup de bancos de dados em VHD(x) que são provisionados no armazenamento NetApp não são suportados.

Máquina	Tipo de armazenamento	Provisione usando	Notas de suporte
VM Hyper-V	Um sistema convidado conetado a SMB3 compartilhamentos residentes em um SVM	Cmdlets SnapCenter GUI ou PowerShell	Suporte apenas para provisionamento. O Hyper-V passa por discos e faz backup de bancos de dados em VHD(x) que são provisionados no armazenamento NetApp não são suportados.

Recomendações de layout de storage para o plug-in SnapCenter para Microsoft SQL Server

Um layout de armazenamento bem projetado permite que o servidor SnapCenter 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 storage para LUNs e discos de máquina virtual (VMDKs) com o plug-in SnapCenter para Microsoft SQL Server instalado no seu ambiente.

Nesse caso, os LUNs podem incluir discos VMware RDM e LUNs iSCSI de conexão direta mapeados para o convidado.

Requisitos de LUN e VMDK

Opcionalmente, você pode usar LUNs ou VMDKs dedicados para obter performance e gerenciamento ideais para os seguintes bancos de dados:

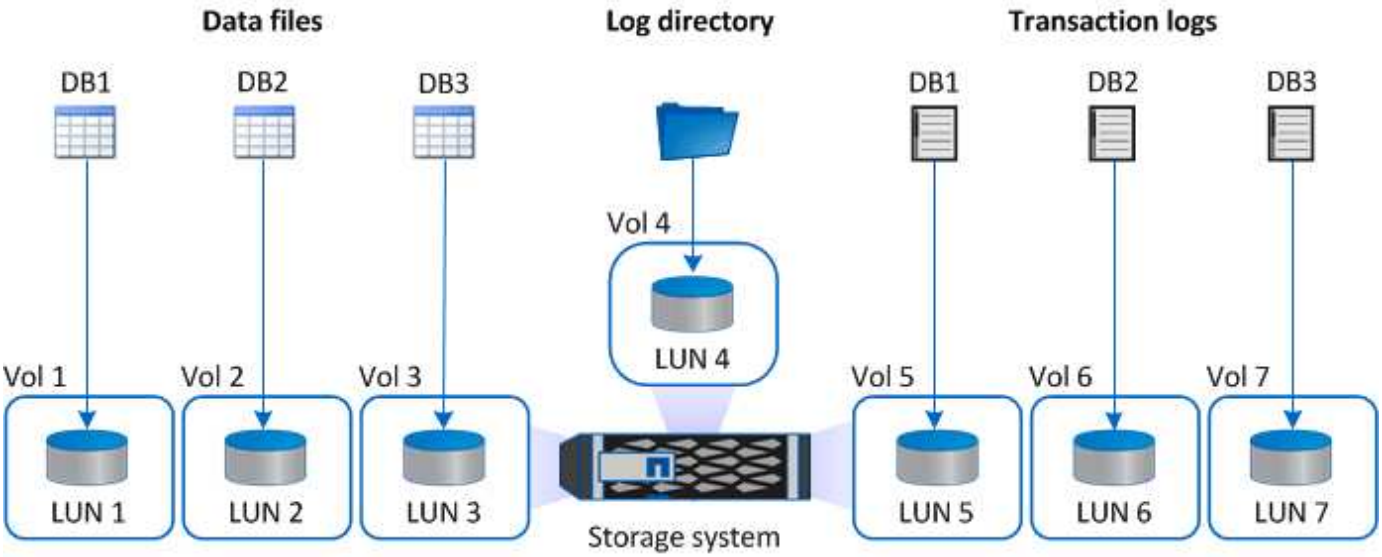
- Bancos de dados de sistemas mestres e de modelos
- Tempdb
- Arquivos de banco de dados do usuário (.mdf e .ndf)
- Arquivos de log de transações de banco de dados do usuário (.ldf)
- Diretório de log

Para restaurar bancos de dados grandes, a prática recomendada é usar LUNs ou VMDKs dedicados. O tempo necessário para restaurar um LUN ou VMDK completo é menor do que o tempo necessário para restaurar os arquivos individuais que são armazenados no LUN ou VMDK.

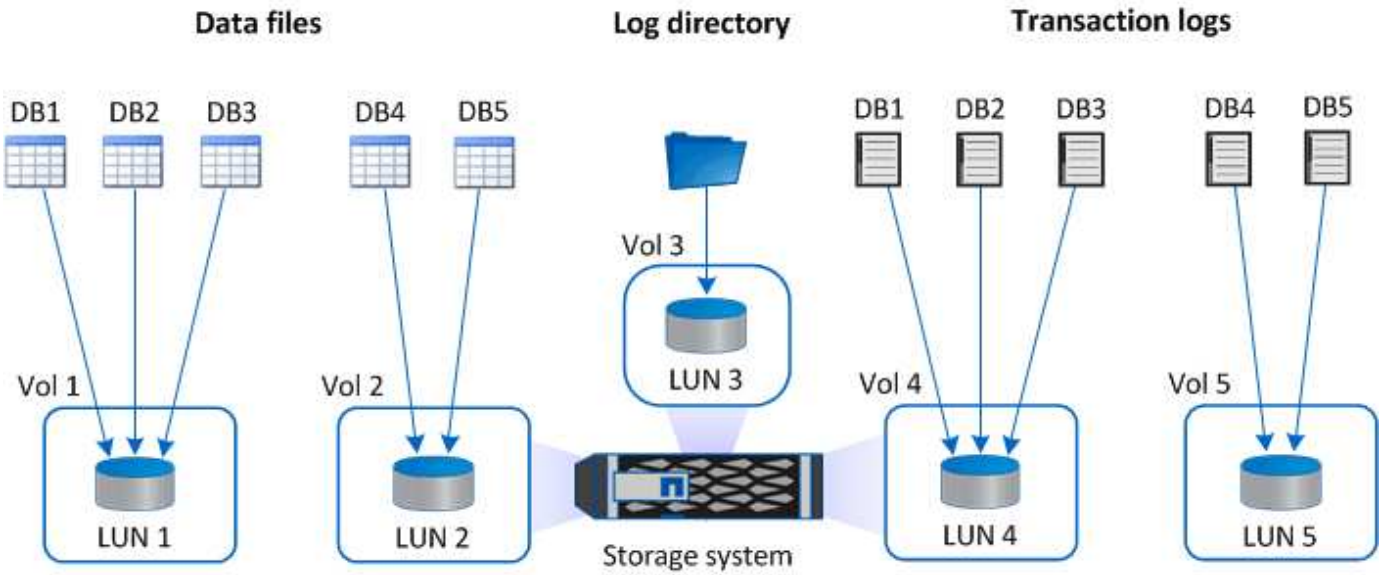
Para o diretório de log, você deve criar um LUN ou VMDK separado para que haja espaço livre suficiente nos discos de arquivo de dados ou log.

Layouts de amostra de LUN e VMDK

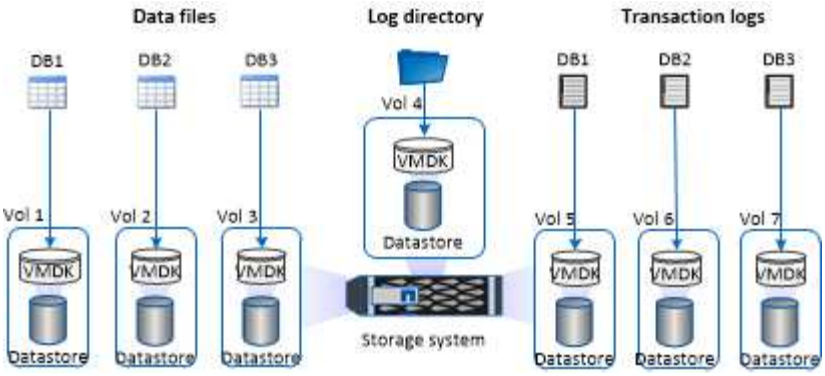
O gráfico a seguir mostra como você pode configurar o layout de armazenamento para bancos de dados grandes em LUNs:



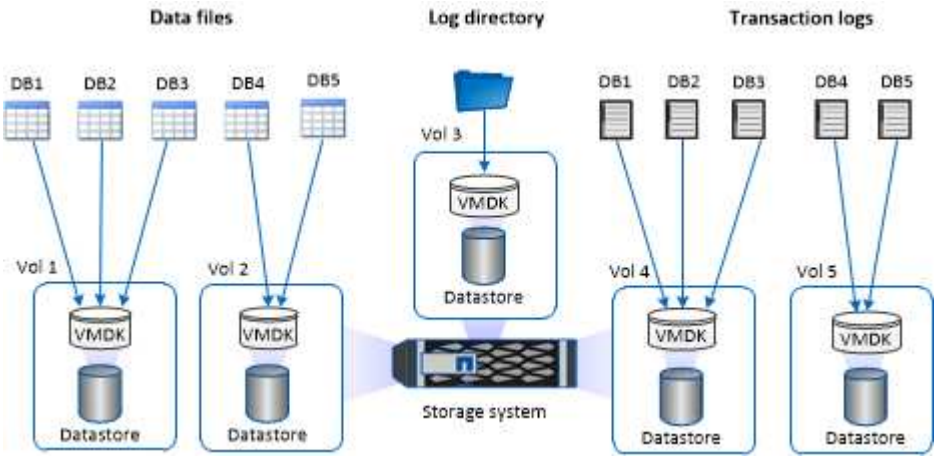
O gráfico a seguir mostra como você pode configurar o layout de armazenamento para bancos de dados médios ou pequenos em LUNs:



O gráfico a seguir mostra como você pode configurar o layout de armazenamento para bancos de dados grandes em VMDKs:



O gráfico a seguir mostra como você pode configurar o layout de armazenamento para bancos de dados médios ou pequenos em VMDKs:



ONTAP Privileges mínimo necessário para plug-in SQL

Os ONTAP Privileges mínimos necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
  - event generate-AutoSupport-log
  - mostra o histórico de trabalhos
  - paragem do trabalho
  - lun
  - lun criar
  - eliminação lun
  - lun igrop add
  - lun igrop criar
  - eliminação do agrupamento lun
  - mudar o nome do grupo lun
  - show de grupos de lun
  - nós complementares de mapeamento de lun
  - mapeamento lun criar

- eliminação do mapeamento lun
- mapeamento lun remove-reporting-nonos
- mostra de mapeamento lun
- modificação de lun
- movimentação de lun no volume
- lun offline
- lun online
- redimensionar lun
- série lun
- mostra lun
- regra adicional de política do SnapMirror
- regra de modificação de política do SnapMirror
- regra de remoção da política do SnapMirror
- SnapMirror policy show
- restauração de SnapMirror
- SnapMirror show
- SnapMirror show-history
- atualização do SnapMirror
- SnapMirror update-ls-set
- SnapMirror lista-destinos
- versão
- clone de volume criar
- show de clone de volume
- início da divisão do clone de volume
- paragem dividida clone volume
- criar volume
- destruição de volume
- clone de arquivo de volume criar
- show-disk-use do arquivo de volume
- volume off-line
- volume online
- modificação do volume
- criar qtree de volume
- eliminação de qtree de volume
- modificação de qtree de volume
- apresentação de qtree de volume
- restrição de volume

- apresentação do volume
- criar instantâneo de volume
- eliminar instantâneo do volume
- modificação do instantâneo do volume
- mudar o nome do instantâneo do volume
- restauração de snapshot de volume
- restauração de arquivo de snapshot de volume
- apresentação de instantâneo do volume
- desmontar o volume
- svm cifs
- compartilhamento cifs de svm criar
- exclusão de compartilhamento cifs de svm
- apresentação do shadowcopy cifs de svm
- exibição de compartilhamento cifs de svm
- mostra cifs de svm
- política de exportação de svm
- criação de política de exportação de svm
- exclusão da política de exportação do svm
- regra de política de exportação de svm criar
- a regra de política de exportação do svm é exibida
- exibição da política de exportação do svm
- svm iscsi
- apresentação da ligação iscsi de svm
- mostra o svm
- interface de rede
- mostra da interface de rede
- svm
- MetroCluster show

Preparar sistemas de storage para replicação SnapMirror e SnapVault para plug-in para SQL Server

Você pode usar um plug-in do 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 disco a disco para conformidade com os padrões e outros fins relacionados à governança. Antes de executar essas tarefas, você deve configurar uma relação de proteção de dados entre os volumes de origem e destino e inicializar a relação.

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 . Se você estiver usando a sincronização ativa do SnapMirror , use os agendamentos padrão do SnapMirror ou SnapVault para a sincronização ativa do SnapMirror e para relacionamentos assíncronos.

Se você estiver vindo para o SnapCenter de um produto NetApp SnapManager e estiver satisfeito com as relações de proteção de dados que configurou, ignore esta seção.

Uma relação de proteção de dados replica dados no storage primário (o volume de origem) para o storage secundário (o volume de destino). Ao inicializar a relação, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não suporta relações em cascata entre volumes SnapMirror e SnapVault (**Primary** > **Mirror** > **Vault**). Você deve usar relacionamentos de fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis de versão e como configurá-los, consulte "Documentação do ONTAP".

Estratégia de backup para recursos do SQL Server

Defina uma estratégia de backup para recursos do SQL Server

Definir uma estratégia de backup antes de criar seus trabalhos de backup ajuda a garantir que você tenha os backups necessários para restaurar ou clonar seus bancos de dados com êxito. Seu Contrato de nível de serviço (SLA), objetivo de tempo de recuperação (rto) e objetivo do ponto de restauração (RPO) determinam em grande parte a sua estratégia de backup.

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados 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 era dos arquivos que precisam ser recuperados do storage de backup para que as operações regulares sejam retomadas após uma falha. O SLA, rto e RPO contribuem para a estratégia de backup.

Tipos de backups suportados

O backup de bancos de dados do sistema e do usuário do SQL Server usando o SnapCenter exige que você escolha o tipo de recurso, como bancos de dados, instâncias do SQL Server e grupos de disponibilidade (AG). A tecnologia Snapshot é utilizada para criar cópias on-line e somente leitura dos volumes nos quais os recursos residem.

Você pode selecionar a opção somente cópia para especificar que o SQL Server não trunca os logs de transação. Você deve usar essa opção quando também estiver gerenciando o SQL Server com outros aplicativos de backup. Manter os logs de transação intactos permite que qualquer aplicativo de backup restaure os bancos de dados do sistema. Os backups somente de cópia são independentes da sequência de backups programados e não afetam os procedimentos de backup e restauração do banco de dados.

Tipo de cópia de segurança	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 transação. O SQL Server trunca os logs de transação removendo as entradas que já estão comprometidas com o banco de dados. Após a conclusão do backup completo, essa opção cria um log de transações que captura informações de transação. Normalmente, você deve escolher essa 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 de sistema mestre e msdb. No entanto, você pode criar backups de log para o banco de dados do sistema modelo.	Faz backup dos arquivos do banco de dados do sistema e dos logs de transação sem truncar os logs. Um backup só de cópia não pode servir como uma base diferencial ou backup diferencial e não afeta a base diferencial. Restaurar um backup completo somente de cópia é o mesmo que restaurar qualquer outro backup completo.
Backup completo do banco de dados	Faz cópias de segurança dos ficheiros da base de dados do sistema. Você pode criar backup completo do banco de dados para bancos de dados de sistema master, model e msdb.	Faz cópias de segurança dos ficheiros da base de dados do sistema.
Backup do log de transações	Faz o backup dos logs de transação truncados, copiando apenas as transações que foram confirmadas desde o backup do log de transação mais recente. Se você agendar backups frequentes de log de transações juntamente com backups completos de bancos de dados, poderá escolher pontos de recuperação granular.	Faz backup dos logs de transação sem truncar-los. Este tipo de cópia de segurança não afeta a sequência de cópias de segurança de registos regulares. Backups de log somente de 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 em políticas; uma programação de backup é especificada na configuração do grupo de recursos. O fator mais crítico na determinação de uma 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 usado a cada hora, enquanto você pode fazer backup de um recurso raramente usado uma vez por dia. Outros fatores incluem a importância do recurso para a sua organização, seu Contrato de nível de Serviço (SLA) e seu objetivo de ponto de recuperação (RPO).

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. Um RPO define a estratégia para a era dos arquivos que precisam ser recuperados do storage 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 usado, não é necessário executar um backup completo mais de uma ou duas vezes por dia. Por exemplo, backups regulares de log de transações podem ser suficientes para garantir que você tenha os backups necessários. Quanto mais você fizer backup de seus bancos de dados, menos Registros de transações que o SnapCenter precisa usar no momento da restauração, o que pode resultar em operações de restauração mais rápidas.

Os programas de backup têm duas partes, como segue:

- Frequência de backup

  A frequência de backup (com que frequência os backups devem ser executados), chamada *schedule type* para alguns plug-ins, faz parte de uma configuração de política. Você pode selecionar a frequência de backup da política por hora, dia, semanal ou mensal. Se você não selecionar nenhuma dessas frequências, a política criada será uma política somente sob demanda. Você pode acessar políticas clicando em **Configurações** > **políticas**.

- Fazer backup de programações

  As agendas 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 que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas. Você pode acessar programações de 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 de que você precisa 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 bancos de dados, o número de tarefas de backup que você escolhe geralmente depende do número de volumes nos quais você colocou seus bancos de dados. Por exemplo, se você colocou um grupo de bancos de dados pequenos em um volume e um banco de dados grande em outro volume, você pode criar um trabalho de backup para os bancos de dados pequenos e um trabalho de backup para o banco de dados grande.

Convenções de nomenclatura de backup para Plug-in para SQL Server

Você pode usar a convenção padrão de nomenclatura Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um carimbo de data/hora aos nomes de Snapshot 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 carimbo de data/hora.

Como alternativa, você pode especificar o formato do nome da captura Instantânea enquanto protege recursos ou grupos de recursos selecionando **usar formato de nome personalizado para cópia Instantânea**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do carimbo de hora é adicionado ao nome do instantâneo.

Opções de retenção de backup para Plug-in para SQL Server

Você pode escolher o número de dias para os quais reter cópias de backup ou especificar o número de cópias de backup que deseja reter, até um máximo de ONTAP de 255 cópias. Por exemplo, sua organização pode exigir que você retenha 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 tiver sido alterado para o grupo de recursos ou recursos, os backups com o rótulo de tipo de agendamento antigo ainda poderão permanecer no sistema.

Para retenção de longo prazo de cópias de backup, você deve usar o backup SnapVault.

Quanto tempo para reter backups de log de transações no sistema de armazenamento de origem

O plug-in do 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 tempo entre dois backups completos.

Por exemplo, se o Plug-in para SQL Server fez um backup completo às 8:00 da manhã e outro backup completo às 5:00 da tarde, ele poderia usar o backup de log de transações mais recente para restaurar o banco de dados a qualquer momento entre as 8:00 da manhã e as 5:00 da tarde se os logs de transação não estiverem disponíveis, o Plug-in para SQL Server pode executar operações de restauração pontual apenas, que restauram um banco de dados para o momento em que o backup completo.

Normalmente, você precisa de operações de restauração mais atualizadas por apenas um dia ou dois. Por padrão, o SnapCenter mantém um mínimo de 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 storage primário ou secundário para Plug-in para SQL Server

É possível verificar cópias de backup no volume de storage primário ou no volume de storage secundário SnapMirror ou SnapVault. A verificação usando um volume de storage secundário reduz a carga no volume de storage primário.

Quando você verifica um backup que está no volume de storage primário ou secundário, todos os snapshots primário e secundário são marcados como verificados.

A licença SnapRestore é necessária para verificar cópias de backup no volume de storage secundário SnapMirror e SnapVault.

Quando agendar trabalhos de verificação

Embora o SnapCenter possa verificar os backups imediatamente após a criação, isso pode aumentar significativamente o tempo necessário para concluir a tarefa de backup e usar muitos recursos. Portanto, é quase sempre melhor agendar a verificação em um trabalho separado para um momento posterior. Por exemplo, se você fizer backup de um banco de dados às 5:00 horas por dia, poderá agendar a verificação para ocorrer uma hora depois às 6:00 horas

Pelo mesmo motivo, geralmente não é necessário executar a verificação de backup toda vez que você executar um backup. Realizar a verificação em intervalos regulares, mas menos frequentes, geralmente é suficiente para garantir a integridade do backup. Um único trabalho de verificação pode verificar vários backups ao mesmo tempo.

Estratégia de restauração para SQL Server

Defina uma estratégia de restauração para o SQL Server

Definir uma estratégia de restauração para o SQL Server permite que você restaure seu banco de dados com sucesso.

Fontes e destinos para uma operação de restauração

É possível restaurar um banco de dados SQL Server a partir de uma cópia de backup em um storage primário ou secundário. Você também pode restaurar o banco de dados para diferentes destinos, além de sua localização original, permitindo que você escolha o destino que atende aos seus requisitos.

Fontes para uma operação de restauração

É possível restaurar bancos de dados do storage 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 para o 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 dentro do mesmo host.
Local 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.

A restauração para host alternativo em servidores ESX para bancos de dados SQL em VMDKs (datastores NFS e VMFS) não é suportada.

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 suporta três tipos de modelos de recuperação de SQL Server:

- Modelo de recuperação simples

  Quando você usa o modelo de recuperação simples, não é possível fazer backup dos logs de transação.

- Modelo de recuperação completo

  Quando você usa o modelo de recuperação completo, você pode restaurar um banco de dados para seu estado anterior a partir do ponto de falha.

- Modelo de recuperação registrado em massa

Quando você usa o modelo de recuperação registrado em massa, você deve executar manualmente a operação registrada em massa. Você deve executar a operação em massa registrada se o log de transações que contém o Registro de confirmação da operação não tiver sido feito backup antes da restauração. Se a operação registrada em massa inserir 10 milhões de linhas em um banco de dados e o banco de dados falhar antes do backup do log de transação, o banco de dados restaurado não conterá as linhas que foram inseridas pela operação registrada 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 mais 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:

- Restauração a partir do storage secundário SnapMirror ou SnapVault
- Restaurar para caminho alternativo (local)

O SnapCenter não é compatível com SnapRestore baseado em volume.

Restaure 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 realiza isso executando a seguinte sequência:

1. Faz o 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 transação que não foram comprometidos com os bancos de dados (incluindo Registros de transações dos backups desde o momento em que o backup foi criado até o momento mais atual).

   Os logs de transações são movidos para frente 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 transação de banco de dados SQL Server a partir de arquivos de backup de envio de log (o envio de log permite enviar automaticamente backups de log de transações de um banco de dados primário em uma instância de servidor primário para um ou mais bancos de dados secundários em instâncias de servidor secundário separadas), você não é capaz de executar uma operação de restauração atualizada dos backups de log de transações. Por esse motivo, você deve usar o SnapCenter para fazer backup de seus arquivos de log de transação de 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 de log de transações do 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 4:00 horas você precisa restaurar a partir de um backup. Por algum motivo, o backup do meio-dia de quarta-feira

falhou a verificação, então você decide restaurar a partir do backup do meio-dia de terça-feira. Depois disso, se o backup for restaurado, todos os logs de transação são movidos para a 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 através do último log de transação escrito na quarta-feira às 4:00 horas (se os logs de transação foram copiados).

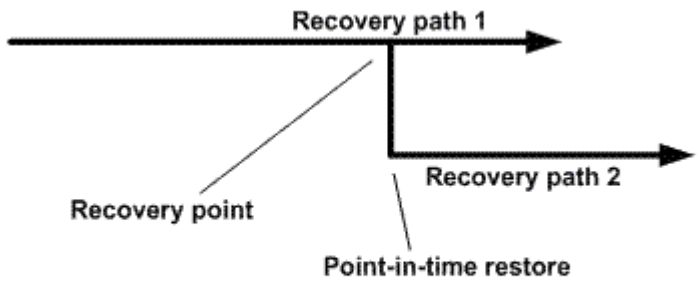
Restaurar para um ponto anterior no tempo

Em uma operação de restauração pontual, os bancos de dados são restaurados apenas para um tempo específico do passado. Uma operação de restauração pontual ocorre nas seguintes situações de restauração:

- O banco de dados é restaurado para um determinado tempo em um log de transação 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 pontual 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 pontual, o que resulta no caminho de recuperação 2. Os novos backups de log de transações são criados sem criar um novo backup completo. Devido a corrupção de dados ou outros problemas, você não pode restaurar o banco de dados atual até que um novo backup completo seja criado. Além disso, não é possível aplicar os logs de transação criados no caminho de recuperação 2 ao backup completo pertencente ao caminho de recuperação 1.

Se você aplicar backups de log de transações, você também pode especificar uma data e hora em particular na qual deseja interromper o aplicativo de transações de backup. Para fazer isso, você especifica uma data e hora dentro do intervalo disponível e o SnapCenter remove quaisquer transações que não foram confirmadas antes desse ponto no tempo. Você pode usar esse método para restaurar bancos de dados a um ponto no tempo antes de uma corrupção ocorrer ou para recuperar de um banco de dados acidental ou exclusão de 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 de log de transações a cada hora. O banco de dados falha às 9:45 da manhã, mas você ainda faz backup dos logs de transação do banco de dados com falha. Você pode escolher entre esses cenários de restauração pontual:

- Restaure o backup completo do banco de dados feito à meia-noite e aceite a perda das alterações feitas posteriormente. (Opção: Nenhuma)
- Restaure o backup completo do banco de dados e aplique todos os backups do log de transações até às 9:45 da manhã (opção: Log até)
- Restaure o backup completo do banco de dados e aplique backups de log de transações, especificando o tempo que você deseja que as transações sejam restauradas a partir do último conjunto de backups de log de transações. (Opção: Por hora específica)

Neste caso, você calcularia a data e a hora em que um determinado erro foi relatado. Quaisquer transações que não tenham sido efetuadas antes da data e hora especificadas são removidas.

Defina uma estratégia de clonagem para o SQL Server

A definição de uma estratégia de clonagem permite clonar seu banco de dados com sucesso.

1. Revise as limitações relacionadas às operações de clone.
2. Decida o tipo de clone que você precisa.

Limitações das operações de clone

Você deve estar ciente das limitações das operações de clone 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 clone estará no estado suspenso quando você executar o comando *renamedg*. Você pode aplicar o Oracle patch 19544733 para corrigir esse problema.
- A clonagem de bancos de dados de um LUN que está diretamente conetado 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 outro host Windows, ou vice-versa, não é suportada.
- O diretório raiz do ponto de montagem do volume não pode ser um diretório partilhado.
- Se você mover um LUN que contém um clone para um novo volume, o clone não poderá ser excluído.

Tipos de operações de clone

Você pode usar o SnapCenter para clonar um backup de banco de dados do SQL Server ou um banco de dados de produção.

- Clonar a partir de um backup de banco de dados

  O banco de dados clonado pode servir como uma linha de base para o desenvolvimento de novos aplicativos e ajudar a isolar erros de aplicativos que ocorrem no ambiente de produção. O banco de dados clonado também pode ser usado para recuperação de erros de banco de dados macio.

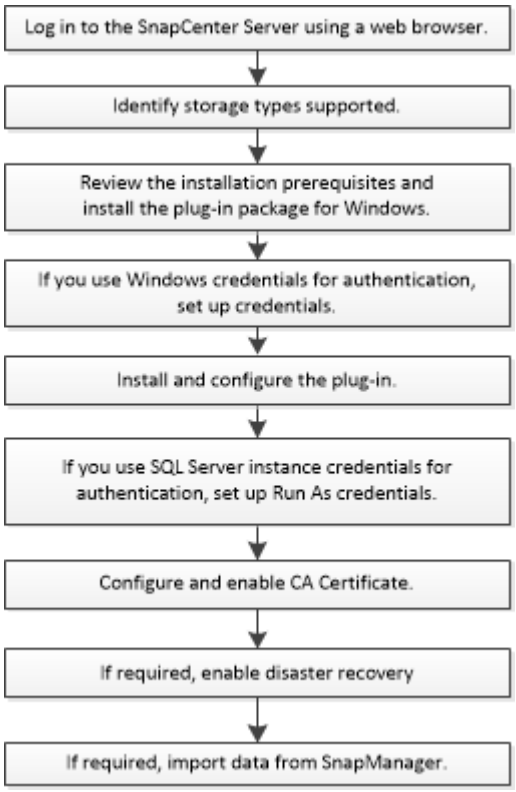
- Ciclo de vida do clone

  Você pode usar o SnapCenter para agendar tarefas de clone recorrentes que ocorrerão quando o banco de dados de produção não estiver ocupado.

Prepare-se para instalar o plug-in do SnapCenter para Microsoft SQL Server

Fluxo de trabalho de instalação para o plug-in SnapCenter para Microsoft SQL Server

Você deve instalar e configurar o plug-in do SnapCenter para o Microsoft SQL Server se quiser proteger bancos de dados do SQL Server.



Pré-requisitos para adicionar hosts e instalar o plug-in do SnapCenter para Microsoft SQL Server

Antes de adicionar um host e instalar os pacotes de plug-ins, você deve completar todos os requisitos.

- Se estiver a utilizar iSCSI, o serviço iSCSI tem de estar em execução.
- Você deve ter um usuário com Privileges de administrador local com permissões de login local no host remoto.
- Se você gerenciar nós de cluster no SnapCenter, precisará ter um usuário com Privileges administrativo para todos os nós do cluster.
- Você deve ter um usuário com permissões sysadmin no SQL Server.

  O plug-in do SnapCenter para Microsoft SQL Server usa o Microsoft VDI Framework, que requer acesso sysadmin.

  "Artigo 2926557: As operações de backup e restauração do SQL Server VDI exigem o sysadmin Privileges"

- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host.
- Se o SnapManager for instalado, você deve ter parado ou desativado o serviço e as programações.

  Se você planeja importar tarefas de backup ou clone para o SnapCenter, não desinstale o SnapManager para o Microsoft SQL Server.

- O host deve ser resolvido para o nome de domínio totalmente qualificado (FQDN) do servidor.

  Se o arquivo hosts for modificado para torná-lo resoluvel e se o nome curto e o FQDN forem especificados no arquivo hosts, crie uma entrada no arquivo SnapCenter hosts no seguinte formato: <ip_address> <host_fqdn> <host_name>

Requisitos de host para instalar o pacote de plug-ins do 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 do sistema host e requisitos de dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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	• .NET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet."

Configure 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 os plug-ins.
- Você deve configurar as credenciais com o Privileges de administrador, incluindo direitos de administrador no host remoto.
- Autenticação SQL em hosts Windows

  Você deve configurar credenciais SQL depois de instalar plug-ins.

  Se você estiver implantando o plug-in do SnapCenter para o Microsoft SQL Server, deverá configurar credenciais SQL após a instalação dos plug-ins. Configure uma credencial para um usuário com permissões sysadmin do SQL Server.

  O método de autenticação SQL é autenticado 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 recursos. Você precisa de 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 **Credential**.
3. Clique em **novo**.
4. Na página Credential (credencial), especifique as informações necessárias para configurar credenciais:

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para a credencial.
Nome de utilizador/Palavra-passe	Introduza o nome de utilizador e a palavra-passe a utilizar para a autenticação. • Administrador de domínio Especifique o administrador de domínio no 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 (apenas para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é: `UserName` Não use aspas duplas (") ou backtick (') nas senhas. Você não deve usar os símbolos menos de (>) e exclamação (!) juntos em senhas. Por exemplo, lessthan!10, lessthan10You!, backtick'12.
Modo de autenticação	Selecione o modo de autenticação que pretende utilizar. Se você selecionar o modo de autenticação SQL, você também deve 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 do SQL Server individual

Você pode configurar credenciais para executar tarefas de proteção de dados em

recursos individuais do SQL Server para cada usuário. Embora você possa configurar as credenciais globalmente, talvez você queira fazer isso apenas para um recurso específico.

Sobre esta tarefa

- Se você estiver usando credenciais do Windows para autenticação, você deve configurar sua credencial antes de instalar plug-ins.

  No entanto, se você estiver usando uma instância do SQL Server para autenticação, você deve adicionar a credencial após a instalação de plug-ins.

- Se você ativou a autenticação SQL durante a configuração das credenciais, a instância descoberta ou o banco de dados será exibida com um ícone de cadeado de cor vermelha.

  Se o ícone de cadeado aparecer, você deve especificar as credenciais da instância ou do banco de dados para adicionar com êxito 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 sysadmin quando as seguintes condições forem atendidas:
  - A credencial é atribuída a uma instância SQL.
  - A instância ou host SQL é atribuída a um usuário RBAC.

    O usuário deve ter o grupo de recursos e o Privileges de backup.

Etapa 1: Adicionar e configurar credenciais

1. No painel de navegação esquerdo, selecione **Configurações**.
2. Na página Configurações, selecione **Credential**.
   a. Para adicionar uma nova credencial, selecione **novo**.
   b. Na página Credential (credencial), configure as credenciais:

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para as credenciais.

Para este campo…	Faça isso…
Nome de utilizador	Introduza o nome de utilizador utilizado para a autenticação do SQL Server. • O administrador de domínio ou qualquer membro do grupo de administradores especificam o administrador do domínio ou qualquer membro do grupo de administradores no sistema no qual você está instalando o plug-in do 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 interno no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo **Username** é: *Username*
Palavra-passe	Introduza a palavra-passe utilizada 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 sysadmin Privileges no servidor SQL.
Host	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 **Resources**.
2. Na página recursos, selecione **Instância** na lista **Exibir**.
   a. Selecione imagem::../media/filter_icon.png[filter icon] e, em seguida, selecione o nome do host para filtrar as instâncias.
   b. Selecione imagem::../media/filter_icon.png[filter icon] para fechar o painel de filtro.
3. Na página proteção de instância, proteja a instância e, se necessário, selecione **Configurar credenciais**.

   Se o usuário que está conetado ao servidor SnapCenter não tiver acesso ao plug-in do SnapCenter para Microsoft SQL Server, o usuário terá que configurar as credenciais.

   A opção credencial não se aplica a bancos de dados e grupos de disponibilidade.

4. Selecione **Atualizar recursos**.

Configure o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite criar uma conta de serviço gerenciado de grupo (gMSA) que fornece gerenciamento automatizado de senha de conta de serviço a partir de uma conta de domínio gerenciado.

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 é um membro do domínio.

Passos

1. Crie uma chave raiz KDS para gerar senhas exclusivas para cada objeto em seu gMSA.
2. Para cada domínio, execute o seguinte comando do 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,…>
.. Execute `Get-ADServiceAccount` o comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Ative o módulo do ative Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando do 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 o host.

b. Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua o Privileges administrativo ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no servidor SnapCenter.

   O servidor SnapCenter 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.

Instale o plug-in do SnapCenter para Microsoft SQL Server

Adicione hosts e instale o pacote de plug-ins do SnapCenter para Windows

Você deve usar a página SnapCenter **Adicionar host** 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 servidor SnapCenter for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deve executar o seguinte:
  - Atualize para o Windows Server 2019 (versão de SO 17763,5936) ou posterior
  - Atualize para o Windows Server 2022 (versão de SO 20348,2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não esteja integrada, desative o UAC no host.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja no estado em execução.

- Se você estiver usando a conta de serviço gerenciado de grupo (gMSA), você deve configurar o gMSA com Privileges administrativo.

  "Configurar conta de serviço gerenciado de grupo no Windows Server 2016 ou posterior para SQL"

Sobre esta tarefa

Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.

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 WSFC (Windows Server failover Clustering), os plug-ins serão instalados em todos os nós do cluster.

Para obter informações sobre como gerenciar hosts, "Gerenciar hosts"consulte .

Passos

1. No painel de navegação esquerdo, selecione **hosts**.
2. Verifique se a guia **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 servidor SnapCenter adiciona o host e, em seguida, instala o plug-in para Windows se o plug-in ainda não estiver instalado no host. Se você selecionar a opção Microsoft SQL Server na página Plug-ins, o servidor SnapCenter instala o plug-in para SQL Server.
Nome do host	Insira 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 adequada do DNS. Portanto, a melhor prática é entrar no FQDN. Você pode inserir os endereços IP ou FQDN de um dos seguintes: • Anfitrião independente • 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 exibir 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.

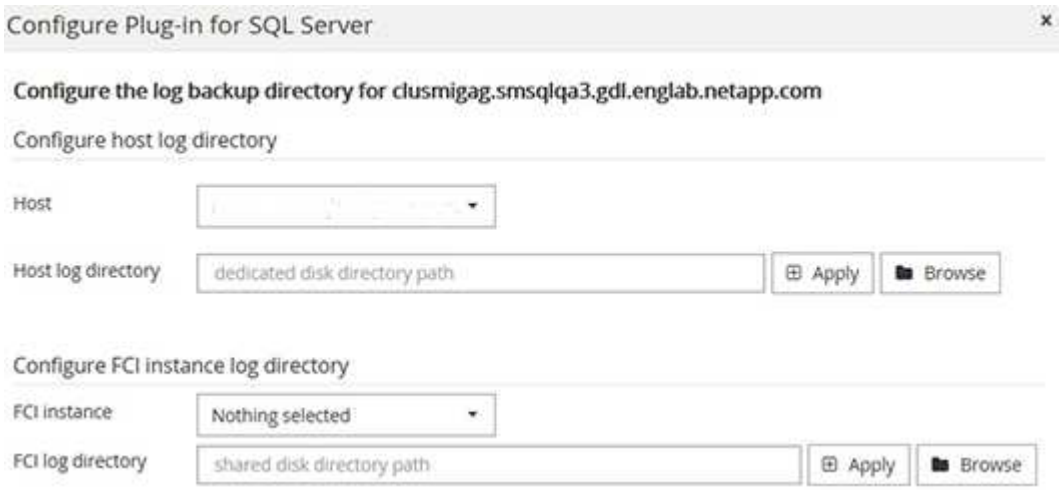
5. Na seção **Select Plug-ins to Install**, selecione os plug-ins a instalar.
6. Selecione **mais opções**.

Para este campo…	Faça isso…
Porta	Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido 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, você deve especificar a mesma porta. Caso contrário, a operação falha.
Caminho de instalação	O caminho padrão é C: Arquivos de programas / NetApp / SnapCenter. Opcionalmente, você pode personalizar o caminho.
Adicione todos os hosts no cluster	Marque essa caixa de seleção para adicionar todos os nós de cluster em um WSFC ou um SQL Availability Group. Você deve adicionar todos os nós de cluster selecionando a caixa de seleção de cluster apropriada na GUI se quiser gerenciar e identificar vários grupos de disponibilidade SQL disponíveis em um cluster.
Ignorar as verificações de pré-instalação	Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

Para este campo…	Faça isso…
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	Marque essa caixa de seleção se quiser usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in. Forneça o nome do gMSA no seguinte formato: Se o host for adicionado com gMSA e se o gMSA tiver login e sys admin Privileges, o gMSA será usado para se conetar à instância SQL.

7. Selecione **Enviar**.
8. Para o SQL Plug-in, 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 execute as seguintes etapas:

      Apenas os LUNs (unidades) NetApp são listados para seleção. O SnapCenter faz o backup e replica o diretório de log do host como parte da operação de backup.



      i. Selecione a letra da unidade ou ponto de montagem no host onde o log do host será armazenado.
      ii. Escolha um subdiretório, se necessário.
      iii. Selecione **Guardar**.
9. Selecione **Enviar**.

   Se você não selecionou 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 .NET, a localização (para plug-ins do Windows) e a versão Java (para plug-ins do Linux) são validados de acordo com os requisitos mínimos. Se os requisitos mínimos não forem cumpridos, são apresentadas mensagens de erro ou de aviso adequadas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado no NetApp SnapCenter para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.

Em uma configuração de HA, se você estiver atualizando o arquivo web.config, será necessário atualizar o arquivo em ambos os nós.

10. Monitorize o progresso da instalação.

Instale o plug-in do SnapCenter para Microsoft SQL Server em vários hosts remotos usando cmdlets

Você pode instalar o plug-in do SnapCenter para Microsoft SQL Server em vários hosts simultaneamente usando o cmdlet Install-SmHostPackage PowerShell.

Antes de começar

Você deve ter feito 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 servidor SnapCenter, estabeleça uma sessão usando o cmdlet Open-SmConnection e insira suas credenciais.
3. Instale o plug-in do SnapCenter 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*. Em alternativa, pode também consultar o "Guia de referência de 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 do SnapCenter para Microsoft SQL Server silenciosamente a partir da linha de comando

Você deve instalar o plug-in do SnapCenter para Microsoft SQL Server a partir da interface de usuário do SnapCenter. No entanto, se você não puder por algum motivo, você pode executar o Plug-in para o programa de instalação do SQL Server sem supervisão no modo silencioso a partir da linha de comando do Windows.

Antes de começar

- Você deve excluir a versão anterior do plug-in do SnapCenter para Microsoft SQL Server antes de instalar.

  Para obter mais informações, "Como instalar um plug-in do SnapCenter manualmente e diretamente do host do plug-in"consulte .

Passos

1. Valide se a pasta C: /Temp existe no host do plug-in e o usuário conetado tem acesso total a ela.
2. Faça o download do plug-in para o software do SQL Server a partir do repositório C:/ProgramData/NetApp/SnapCenter/Package.

   Este caminho é acessível a partir do host onde o servidor SnapCenter 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 para o qual 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 marcador de posição pelos dados

   - Debug_Log_Path é o nome e a localização 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.
   - Domínio/administrador é a conta do serviço Web do SnapCenter Plug-in para Microsoft Windows.
   - Senha é a senha para a conta de serviço da Web do SnapCenter Plug-in para Microsoft Windows. E `"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 são sensíveis a maiúsculas e 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 do 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 servidor SnapCenter. Você pode Registrar o plug-in no servidor SnapCenter adicionando o host usando a GUI do SnapCenter ou 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

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso

- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
   a. Clique em **filtro**.
   b. Opcional: Especifique a data de início e fim.
   c. No menu suspenso tipo, selecione **Instalação 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 **Visualizar logs**.

Configurar certificado CA

Gerar arquivo CSR do 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 a CSR gerada. O certificado terá uma chave privada associada a ele.

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

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

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

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

Para configurações de cluster, o nome do cluster (FQDN de cluster virtual) e os respetivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome alternativo (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados CA

Você deve importar os certificados de CA para o servidor SnapCenter e os plug-ins de

host do Windows usando o MMC (console de gerenciamento da Microsoft).

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 **Yes**, importe a chave privada e clique em **Next**.
Importar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

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

7. Repita o passo 5 para a pasta "Pessoal".

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia 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 **thumbprint**.
   d. Copie os carateres 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

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.

Configure o certificado CA com os serviços de plug-in do host do Windows

Você deve configurar o certificado CA com os serviços de plug-in host do Windows para ativar o certificado digital instalado.

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, 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"
   ```

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet RUN *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando as *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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- * * Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da 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 são concluídas com êxito.

Configurar a recuperação de desastres

Recuperação de desastres do plug-in SnapCenter para SQL Server

Quando o plug-in do SnapCenter estiver inativo, siga 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 principal.
- Envie o plug-in do SnapCenter para SQL Server para um host alternativo usando a página **Adicionar host** ou **Modificar host**. Consulte "Gerenciar hosts" para obter mais informações.

Passos

1. Selecione o host na página **hosts** para modificar e instalar o plug-in do SnapCenter para SQL Server.
2. (Opcional) substitua o plug-in do SnapCenter para arquivos de configuração do SQL Server do backup de recuperação de desastres (DR) para a nova máquina.
3. Importe programações do Windows e SQL da pasta do plug-in do SnapCenter para SQL Server do backup de DR.

Informações relacionadas

Veja "APIs de recuperação de desastres"o vídeo.

Recuperação de desastres de storage (DR) para plug-in SnapCenter para SQL Server

Você pode recuperar o plug-in do 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 estão no modo de manutenção.
- Quebre a relação SnapMirror/SnapVault. "Quebrando relacionamentos SnapMirror"
- Conete o LUN do secundário à máquina host com a mesma letra de unidade.
- Certifique-se de que todos os discos estejam conetados usando as mesmas letras de unidade usadas antes do DR.
- Reinicie o serviço de servidor MSSQL.
- Certifique-se de que os recursos SQL estão novamente online.

Sobre esta tarefa

A recuperação de desastres (DR) não é compatível com 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 a tarefa DR está ativada ou não clicando em **Monitor** > **jobs**.

Depois de terminar

- Se novos bancos de dados forem criados após o failover, os bancos de dados 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 o plug-in do SnapCenter para backups do SQL Server criados durante o failover usando a IU ou o cmdlet a seguir: `Remove-SmBackup`
- Após o failover, se você quiser que alguns dos recursos estejam em modo não DR, use o seguinte cmdlet: `Remove-SmResourceDRMode`

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

- O servidor SnapCenter gerenciará os recursos de storage individuais (bancos de dados SQL) que estão no modo DR ou não DR, mas não o grupo de recursos com recursos de storage que estão no modo DR ou no modo não DR.

Failback do plug-in do SnapCenter para storage secundário do SQL Server para storage primário

Depois que o plug-in do SnapCenter para o armazenamento primário do SQL Server estiver novamente on-line, você deve fazer o failback para o storage primário.

Antes de começar

- Coloque o plug-in do SnapCenter para SQL Server no modo **Manutenção** na página hosts gerenciados.
- Desconete o storage secundário do host e conete-se ao storage primário.
- Para fazer o failback para o storage primário, verifique se a direção da relação permanece a mesma 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 novamente a operação de ressincronização reversa.

  Para obter mais informações, consulte "Reverter a ressincronização das relações de espelho"

- Reinicie o serviço de servidor MSSQL.
- Certifique-se de que os recursos SQL estão novamente online.

> 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 subsequente do host.

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 a tarefa DR está ativada ou não clicando em **Monitor** > **jobs**.

Depois de terminar

Você pode excluir o plug-in do SnapCenter para backups do SQL Server criados durante o failover usando a IU ou o cmdlet a seguir: `Remove-SmDRFailoverBackups`

Instale o plug-in do SnapCenter para VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs) ou se você quiser proteger VMs e datastores, você deverá implantar o plug-in do SnapCenter para o dispositivo virtual VMware vSphere.

Para obter informações sobre como implantar, "Visão geral da implantação" consulte .

Implantar certificado CA

Para configurar o certificado CA com o plug-in SnapCenter para VMware vSphere, "Criar ou importar certificado SSL" consulte .

Configure o arquivo CRL

O plug-in do SnapCenter para VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL para o plug-in do SnapCenter para 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.

Preparar-se para a proteção de dados

Pré-requisitos para usar o plug-in do SnapCenter para Microsoft SQL Server

Antes de começar a usar o plug-in para SQL Server, o administrador do SnapCenter deve instalar e configurar o servidor SnapCenter e executar tarefas pré-requisitos.

- Instalar e configurar o servidor SnapCenter.
- Inicie sessão no SnapCenter.
- Configure o ambiente SnapCenter adicionando ou atribuindo conexões do sistema de storage e criando credenciais.

> O SnapCenter não é compatível com vários SVMs com o mesmo nome em clusters diferentes. Cada SVM com suporte do SnapCenter precisa 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 NetApp ou vice-versa executando invoke-SmConfigureResources.

  Para obter informações sobre como executar o cmdlet, consulte "Guia de referência de cmdlet do software SnapCenter"

- Se você estiver usando o servidor SnapCenter para proteger bancos de dados SQL que residem em LUNs ou VMDKs do VMware RDM, você deverá implantar o plug-in do SnapCenter para VMware vSphere e Registrar o plug-in com o SnapCenter. A documentação do plug-in do SnapCenter para VMware vSphere tem mais informações.

  "Plug-in do SnapCenter para documentação do VMware vSphere"

- Execute o provisionamento de storage no lado do host usando o plug-in do SnapCenter para Microsoft Windows.
- Configure as relações do SnapMirror e do SnapVault, se quiser fazer backup da replicação.

Para obter detalhes, consulte informações de instalação do SnapCenter.

Para usuários do SnapCenter 4.1.1, a documentação do plug-in do SnapCenter para VMware vSphere 4.1.1 tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos. Para usuários do SnapCenter 4,2.x, o Agente de dados do NetApp 1,0 e 1,0.1, a documentação tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in do SnapCenter para 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 plug-in do SnapCenter para VMware vSphere 4,3 tem informações sobre como proteger bancos de dados virtualizados e sistemas de

arquivos usando o plug-in SnapCenter baseado no Linux para o dispositivo virtual VMware vSphere (formato Open Virtual Appliance).

"Plug-in do SnapCenter para documentação do VMware vSphere"

Como recursos, grupos de recursos e políticas são usados para proteger o SQL Server

Antes de usar o SnapCenter, é útil entender 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 clone com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host ou cluster.

  Quando você executa uma operação em um grupo de recursos, executa essa operação nos recursos definidos no grupo de recursos de acordo com a programação especificada para o grupo de recursos.

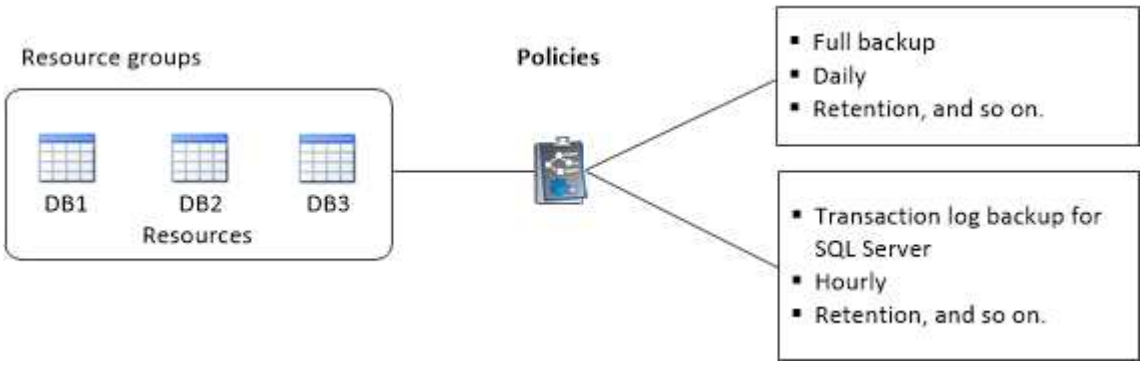
  Você pode fazer backup sob demanda de um único recurso ou de um grupo de recursos. Você também pode executar backups programados para recursos únicos e grupos de recursos.

- As políticas especificam a frequência de backup, retenção de cópia, 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 quando você executa um backup sob demanda para um único recurso.

Pense em um grupo de recursos como definindo *o que* você quer proteger e quando você quer protegê-lo em termos de dia e tempo. Pense em uma política como definindo *como* você quer protegê-la. Se você estiver fazendo backup de todos os bancos de dados ou fazendo backup de todos os sistemas de arquivos de um host, por exemplo, você pode criar um grupo de recursos que inclua todos os bancos de dados ou todos os sistemas de arquivos no host. Em seguida, você pode anexar duas políticas ao grupo de recursos: Uma política diária e uma política por hora. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diário e outro agendamento que executa backups de log por hora.

A imagem a seguir ilustra a relação entre recursos, grupos de recursos e políticas para bancos de dados:



Faça backup do banco de dados do SQL Server, instância ou grupo de disponibilidade

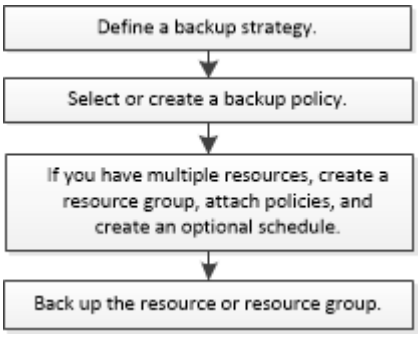
Fluxo de trabalho de backup

Ao instalar o plug-in do SnapCenter 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 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 desativadas se você selecionar um LUN que não seja NetApp, um banco de dados corrompido ou um banco de dados que está sendo restaurado.

Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração, recuperação, verificação e clone. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte o. "Guia de referência de 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 snapshots dos bancos de dados.

Quando você seleciona um banco de dados para um backup completo do banco de dados na página recursos, o SnapCenter seleciona automaticamente todos os outros bancos de dados que residem no mesmo volume de storage. Se o LUN ou VMDK armazenar apenas um único banco de dados, você pode limpar ou reselecionar o banco de dados individualmente. Se o LUN ou VMDK contiver vários bancos de dados, você deve limpar ou reselecionar 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 divididos por 35.

Você pode configurar o número máximo de bancos de dados para cada Snapshot na política de backup.

Quando o SnapCenter cria um instantâneo, todo o volume do sistema de storage é capturado no instantâneo. No entanto, o backup é válido apenas para o servidor host SQL para o qual o backup foi criado.

Se os dados de outros servidores host SQL residirem no mesmo volume, esses dados não poderão ser restaurados a partir do Snapshot.

Encontre mais informações

"Operações de quiesce ou agrupamento de recursos falham"

Determine se os recursos estão disponíveis para backup

Os recursos são bancos de dados, instâncias de aplicativos, grupos de disponibilidade e componentes semelhantes que são mantidos pelos plug-ins instalados. Você pode adicionar esses recursos a grupos de recursos para que você possa executar tarefas de proteção de dados, mas primeiro você deve identificar quais recursos você tem disponíveis. A determinação dos recursos disponíveis também verifica se a instalação do plug-in foi concluída com êxito.

Antes de começar

- Você já deve ter concluído tarefas como instalar o servidor SnapCenter, adicionar hosts, criar conexões do sistema de storage e adicionar credenciais.
- Para descobrir os bancos de dados Microsoft SQL, uma das seguintes condições deve ser atendida.
  - O usuário que foi usado para adicionar o host de plug-in ao servidor SnapCenter deve ter as permissões necessárias (sysadmin) no Microsoft SQL Server.
  - Se a condição acima não for atendida, no servidor SnapCenter você deve configurar o usuário que tem as permissões necessárias (sysadmin) no Microsoft SQL Server. O usuário deve ser configurado no nível de instância do Microsoft SQL Server e o usuário pode ser um usuário SQL ou Windows.
- Para descobrir os bancos de dados Microsoft SQL em um cluster do Windows, você deve desbloquear a porta TCP/IP de instância de cluster de failover (FCI).
- Se os bancos de dados residirem em LUNs ou VMDKs do VMware RDM, você deverá implantar o plug-in do SnapCenter para VMware vSphere e Registrar o plug-in no SnapCenter.

  Para obter mais informações, consulte "Implante o plug-in do SnapCenter para VMware vSphere"

- Se o host for adicionado com gMSA e se o gMSA tiver login e administrador do sistema Privileges, o gMSA será usado para se conetar à instância 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 **Estado geral** está definida como não disponível para cópia de segurança quando qualquer uma das seguintes situações for verdadeira:

- Os bancos de dados não estão em um LUN NetApp.
- Os bancos de dados não estão no estado normal.

  Os bancos de dados não estão no estado normal quando estão offline, restaurando, recuperando pendente, suspeitando, etc.

- Os bancos de dados não têm Privileges suficientes.

Por exemplo, se um usuário tiver acesso somente à base de dados, os arquivos e propriedades do banco de dados não podem ser identificados e, portanto, não podem ser copiados.

O SnapCenter só pode fazer backup do banco de dados principal se você tiver uma configuração de grupo de disponibilidade no SQL Server Standard Edition.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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. Em seguida, pode 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 servidor SnapCenter.

   Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

   Os recursos são exibidos juntamente com informações como tipo de recurso, nome de 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` será exibido na coluna **Estado geral**.

     Não é possível executar operações de proteção de dados em um banco de dados que esteja em um storage que não seja NetApp.

   - Se o banco de dados estiver em um armazenamento NetApp e não estiver protegido, `Not protected` será exibido na coluna **Estado geral**.
   - Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, a interface do usuário exibirá `Backup not run` a mensagem na coluna **Estado 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` a mensagem na coluna **Estado geral**.

   Se você ativou uma autenticação SQL ao configurar as credenciais, a instância descoberta ou banco de dados será exibida com um ícone de cadeado vermelho. Se o ícone de cadeado aparecer, você deve especificar as credenciais da instância ou do banco de dados para adicionar com êxito a instância ou o banco de dados a um grupo de recursos.

1. Depois que o administrador do SnapCenter atribuir os recursos a um usuário do RBAC, o usuário do RBAC deve fazer login e clicar em **Atualizar recursos** para ver o status geral mais recente dos recursos.

Migrar recursos para o sistema de storage NetApp

Depois de ter provisionado o sistema de armazenamento NetApp usando o plug-in

SnapCenter para Microsoft Windows, você pode migrar seus recursos para o sistema de armazenamento NetApp ou de um LUN NetApp para outro LUN NetApp usando a interface gráfica do usuário (GUI) do SnapCenter ou usando os cmdlets do PowerShell.

Antes de começar

- Você deve ter adicionado sistemas de storage ao servidor SnapCenter.
- Você deve ter atualizado (descoberto) os recursos do SQL Server.

A maioria dos campos nessas páginas do assistente são auto-explicativos. 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 **Resources** 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 **Migrate**.
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, você deve selecionar os bancos de dados dessa instância na lista suspensa **bancos de dados**.
Escolha Destinos	Selecione o local de destino para dados e arquivos de log. Os ficheiros de dados e de registo são movidos para a pasta dados e Registo, respetivamente, sob a unidade NetApp selecionada. Se qualquer 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**.
Opções	Selecione **Excluir cópia do banco de dados migrado no local original** para excluir a cópia do banco de dados da origem. Opcional: **EXECUTE ESTATÍSTICAS DE ATUALIZAÇÃO em 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 de 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.
• DBCC CHECKDB opções*	• Selecione a opção **PHYSICAL_only** para limitar a verificação de integridade à estrutura física do banco de dados e para detetar páginas rasgadas, falhas na 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 do SQL Server usa o Microsoft SQL Server Database Consistency Checker (DBCC) para verificar a integridade física e lógica dos objetos no banco de dados. Você pode querer selecionar essa opção para diminuir o tempo de execução. • Selecione **TABLOCK** opção para limitar as verificações e obter bloqueios em vez de usar um instantâneo de banco de dados interno.

6. Revise o resumo e clique em **concluir**.

Criar políticas de backup para bancos de dados do SQL Server

Você pode criar uma política de backup para o recurso ou para o grupo de recursos antes de usar o SnapCenter para fazer backup de recursos do SQL Server ou criar uma política de backup no momento em que criar um grupo de recursos ou fazer backup de um único recurso.

Antes de começar

- Você precisa ter definido sua estratégia de proteção de dados.
- Você precisa se preparar para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, identificar recursos e criar conexões do sistema de storage.
- Você deve ter configurado o diretório de log do host para o backup de log.
- Você deve ter atualizado (descoberto) os recursos do SQL Server.

- Se você estiver replicando snapshots em um espelhamento ou cofre, o administrador do SnapCenter deverá ter atribuído as máquinas virtuais de storage (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 false.

- Reveja os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror. Para obter informações, "Limites de objetos para sincronização ativa do SnapMirror" consulte .

Sobre esta tarefa

- Uma política de backup é um conjunto de regras que regem como você gerencia e retém backups e com que frequência o backup do recurso ou do grupo de recursos é feito. Além disso, você pode especificar as configurações de replicação e script. Especificar opções em uma política economiza tempo quando você deseja reutilizar a política para outro grupo de recursos.

  O SCRIPT_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 usar o caminho padrão para segurança.

  O valor da chave pode ser exibido do swagger através 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 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.

    Especificar um período de bloqueio instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na política.

    Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

    As configurações do SnapLock primário são gerenciadas na política de backup do SnapCenter e as configurações do SnapLock secundário são gerenciadas pelo ONTAP.

Passo 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 a descrição da política.

Passo 2: Configurar opções de backup

1. Escolha seu tipo de backup

Backup completo e backup de log

Faça backup dos arquivos de banco de dados e logs de transação e truncar os logs de transação.

1. Selecione **cópia de segurança completa e cópia de segurança de registo**.
2. 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 uma cópia de segurança dos ficheiros da base de dados.

1. Selecione **cópia de segurança completa**.
2. 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

1. Faça backup dos logs de transação.
2. Selecione **Log backup**.

Cópia de segurança apenas

1. Se você estiver fazendo backup de seus recursos usando outro aplicativo de backup, selecione **Backup somente cópia**.

Manter os logs de transação intactos permite que qualquer aplicativo de backup restaure os bancos de dados. Você normalmente não deve usar a opção somente cópia em nenhuma outra circunstância.

> O Microsoft SQL não suporta a opção **cópia apenas de backup** juntamente com a opção **backup completo e backup de log** para armazenamento secundário.

1. Na seção Configurações do Grupo de disponibilidade, execute as seguintes ações:

   a. Backup apenas na réplica de backup preferencial.

      Selecione esta opção para fazer backup apenas na réplica de backup preferida. A réplica de backup preferida é decidida pelas preferências de backup configuradas para o AG no SQL Server.

   b. Selecione réplicas para backup.

Escolha a réplica AG primária ou a réplica AG secundária para o backup.

c. Selecionar prioridade de cópia de segurança (prioridade mínima e máxima de cópia de segurança)

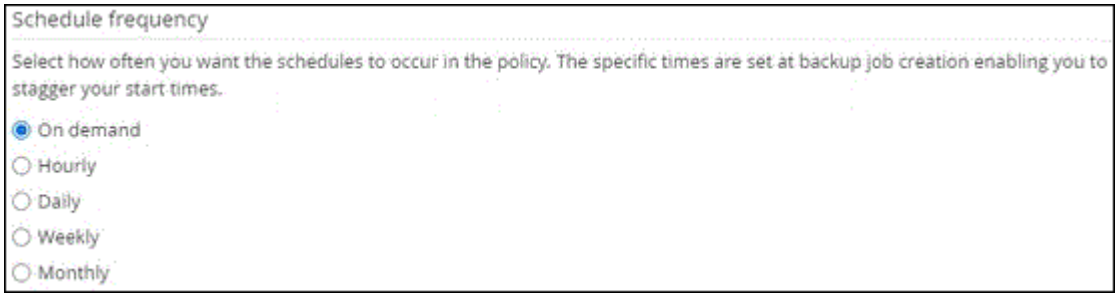
Especifique um número mínimo de prioridade de backup e um número máximo de prioridade de backup que decida a réplica AG para backup. Por exemplo, você pode ter uma prioridade mínima de 10 e uma prioridade máxima de 50. Neste caso, todas as réplicas AG com uma prioridade superior a 10 e inferior a 50 são consideradas para backup.

Por padrão, a prioridade mínima é 1 e a prioridade máxima é 100.

Nas 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 apenas no nível do nó.

2. Programe a frequência de backup para esta política. Especifique o tipo de agendamento selecionando **on demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.

Você só pode selecionar um tipo de agendamento para uma política.



Você pode especificar a programação (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 atribuir diferentes programações de backup a cada política.

Se você tiver agendado para as 2:00 da manhã, o horário não será acionado durante o horário de verão (DST).

Etapa 3: Configurar as configurações de retenção

Na página retenção, dependendo do tipo de backup selecionado na página tipo de backup, execute uma ou mais das seguintes ações:

1. Na seção Configurações de retenção para a operação de restauração de até o minuto, execute uma das seguintes ações:

Número específico de cópias

Guarde apenas um número específico de instantâneos.

1. Selecione a opção **manter backups de log aplicáveis aos últimos dias do <number>** e especifique o número de dias a serem retidos. Se você estiver perto desse limite, talvez queira excluir cópias mais antigas.

Número específico de dias

Guarde as cópias de backup por um número específico de dias.

1. Selecione a opção **manter backups de log aplicáveis aos últimos dias do <number> de backups completos** e especifique o número de dias para manter as cópias de backup de log.

1. Na seção **Configurações completas de retenções de backup** para as configurações de retenção sob demanda, execute as seguintes ações:
   a. Especifique o número total de instantâneos a manter
      i. Para especificar o número de instantâneos a serem mantidos, selecione **Total de cópias Snapshot a serem mantidas**.
      ii. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas 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 snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino.

O valor máximo de retenção é 1018 para recursos no ONTAP 9.4 ou posterior e 254 para recursos no ONTAP 9.3 ou anterior. Os backups falharão se a retenção for definida para um valor maior do que o que a versão subjacente do ONTAP suporta.

1. Período de tempo para manter instantâneos
   a. Se você quiser especificar o número de dias para os quais deseja manter as capturas instantâneas antes de excluí-las, selecione **manter cópias snapshot para**.
2. Se desejar especificar o período de bloqueio de instantâneos, selecione **período de bloqueio de cópias instantâneas** e selecione dias, meses ou anos.

   O período de retenção do SnapLock deve ser inferior a 100 anos.

3. Na seção **Configurações completas de retenções de backup** para as configurações de retenção horária, diária, semanal e mensal, especifique as configurações de retenção para o tipo de agendamento selecionado na página tipo de backup.
   a. Especifique o número total de instantâneos a manter
      i. Para especificar o número de instantâneos a serem mantidos, selecione **Total de cópias Snapshot a serem mantidas**. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro.

Você deve definir a contagem de retenção como 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino.

1. Período de tempo para manter instantâneos
   a. Para especificar o número de dias para os quais você deseja manter os instantâneos antes de excluí-los, selecione **manter cópias snapshot para**.
2. Se desejar especificar o período de bloqueio de instantâneos, selecione **período de bloqueio de cópias instantâneas** e selecione dias, meses ou anos.

   O período de retenção do SnapLock deve ser inferior a 100 anos.

   Por padrão, a retenção de instantâneos de log é definida como 7 dias. Use o cmdlet Set-SmPolicy para alterar a retenção de Snapshot de log.

Este exemplo define a retenção de instantâneos de log como 2:

Exemplo 1. Mostrar exemplo

```
Set-SmPolicy -policyname 'newpol' -PolicyType 'Backup' -PluginPolicyType 'SCSQL' -sqlbackuptype
'FullBackupAndLogBackup' -RetentonSettings 2 [BackupType] [DADOS];ScheduleType
'Hourly';RetentyType 2 2
```

"O SnapCenter retém cópias Snapshot do banco de dados"

Etapa 4: Configurar as configurações de replicação

1. Na página replicação, especifique a replicação para o sistema de storage secundário:

Atualize o SnapMirror

Atualize o SnapMirror depois de criar uma cópia Snapshot local.

1. Selecione esta opção para criar cópias espelhadas de conjuntos de backup em outro volume (SnapMirror).

   Esta opção deve estar ativada para a 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.

   "Veja os backups e clones do SQL Server na página topologia"Consulte .

Atualize o SnapVault

Atualize o SnapVault depois de criar uma cópia 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 apenas no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página topologia atualiza o período de bloqueio no secundário que é recuperado do ONTAP.

   Para obter mais informações sobre o SnapLock Vault, consulte "Armazene cópias Snapshot em WORM em um destino de cofre"

   "Veja os backups e clones do SQL Server na página topologia"Consulte .

Etiqueta de política secundária

1. Selecione uma etiqueta Snapshot.

Dependendo do rótulo de captura instantânea selecionado, o ONTAP aplica a política de retenção de snapshot secundária que corresponde ao rótulo.

> Se você selecionou **Atualizar SnapMirror depois de criar uma cópia Snapshot local**, você pode especificar opcionalmente o rótulo de política secundária. No entanto, se você selecionou **Atualizar SnapVault depois de criar uma cópia Snapshot local**, especifique o rótulo de política secundária.

Contagem de tentativas de erro

1. Insira o número de tentativas de replicação que devem ocorrer antes que o processo pare.

Passo 5: Configurar definições de script

1. Na página Script, insira o caminho e os argumentos do prescritor ou postscript que devem ser executados antes ou depois da operação de backup, respetivamente.

Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas e enviar logs.

O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

Você deve configurar a política de retenção SnapMirror no ONTAP para que o storage secundário não atinja o limite máximo de snapshots.

Etapa 6: Configurar as configurações de verificação

Na página Verificação, execute as seguintes etapas:

1. Na seção Executar verificação para as seguintes programações de backup, selecione a frequência de agendamento.
2. Na seção Opções de verificação consistência de banco de dados, execute as seguintes ações:
   a. Limitar a estrutura de integridade à estrutura física do banco de dados (FÍSICO_SOMENTE)
      i. Selecione **Limit 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 para detetar páginas rasgadas, falhas de checksum e falhas comuns de hardware que afetam o banco de dados.
   b. Suprimir todas as mensagens de informação (SEM INFOMSGS)
      i. Selecione **Suprima todas as mensagens de informação (NO_INFOMSGS)** para suprimir todas as mensagens informativas. Selecionado por predefinição.
   c. Exibir todas as mensagens de erro reportadas 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 verifique índices não agrupados (NOINDEX)** se você não quiser verificar índices não agrupados. O banco de dados do SQL Server usa o Microsoft SQL Server Database Consistency Checker (DBCC) para verificar a integridade física e lógica dos objetos no banco de dados.
   e. Limitar as verificações e obter os bloqueios em vez de usar um instantâneo de banco de dados interno (TABLOCK)
      i. Selecione **Limit as verificações e obtenha os bloqueios em vez de usar uma cópia Snapshot do banco de dados interno (TABLOCK)** para limitar as verificações e obter 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 prescritor ou postscript que devem ser executados antes ou depois da operação de verificação, respetivamente.

O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

Passo 7: Rever resumo

1. Revise o resumo e selecione **Finish**.

Crie grupos de recursos e anexe políticas para o SQL Server

Um grupo de recursos é um contentor ao qual você adiciona recursos que deseja fazer backup e proteger juntos. Um grupo de recursos permite fazer 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 tarefa 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 a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.
- A adição de novos bancos de dados sem a sincronização ativa do SnapMirror a um grupo de recursos existente que contenha recursos com a sincronização ativa do SnapMirror não é suportada.
- A adição de novos bancos de dados a um grupo de recursos existente no modo failover da sincronização ativa do SnapMirror não é suportada. Você pode adicionar recursos ao grupo de recursos apenas no estado regular ou de failback.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** na lista **Exibir**.

   Se você recentemente adicionou um recurso ao SnapCenter, clique em **Atualizar recursos** para exibir 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	Introduza o nome do grupo de recursos. O nome do grupo de recursos não deve exceder 250 carateres.

Para este campo…	Faça isso…
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.
Use o formato de nome personalizado para cópia Snapshot	Opcional: Insira um nome e formato personalizados do instantâneo. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

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 tiver adicionado recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois de atualizar sua lista de recursos.

   b. Para mover recursos da seção **recursos disponíveis** para a seção recursos selecionados, execute uma das seguintes etapas:
      - Selecione **seleção automática de 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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Na seção Configurar agendas para políticas selecionadas, clique em + na coluna Configurar agendas para a política para a qual você deseja configurar o agendamento.
   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação especificando a data de início, data de expiração e frequência e clique em **OK**.

      Você deve fazer isso para cada frequência listada na política. As programações configuradas são listadas na coluna agendas aplicadas na seção **Configurar programações 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 é o agendador do Microsoft Windows.

As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas de backup do SnapCenter. Você não deve modificar as programações e renomear a tarefa de backup criada no Windows Scheduler ou no SQL Server Agent.

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 está hospedando o banco de dados principal.

   a. Clique em **Load Locators** para carregar os volumes SnapMirror e SnapVault para executar a verificação no armazenamento secundário.
   b. Selecione a política para a qual pretende configurar o seu agendamento de verificação e, em seguida, clique em * * .
   c. Na caixa de diálogo Adicionar agendamentos de verificação policy_name , execute as seguintes ações:

Se você quiser…	Faça isso…
Execute a verificação após a cópia de segurança	Selecione **Executar verificação após backup**.
Marque uma verificação	Selecione **Executar verificação agendada**.

   d. Clique em **OK**.

      As programações configuradas são listadas na coluna agendas aplicadas. Pode rever e editar clicando em * ou eliminar 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 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-SmtpServer.

9. Revise o resumo e clique em **Finish**.

Informações relacionadas

"Criar políticas de backup para bancos de dados do SQL Server"

Requisitos para fazer backup de recursos SQL

Antes de fazer backup de um recurso SQL, você deve garantir que vários requisitos sejam atendidos.

- Você precisa ter migrado um recurso de um sistema de storage que não seja da NetApp para um sistema de storage da NetApp.
- Você deve ter criado uma política de backup.
- Se você quiser fazer backup de um recurso que tenha uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.
- A operação de backup iniciada por um usuário de diretório ativo (AD) falha se a credencial de 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 pode ser acionada tarde 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 Administrador da infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estão em andamento.

  As instalações de plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento, pois 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 do sistema de armazenamento devem ser exclusivos.

  O SnapCenter não é compatível com vários sistemas de storage com o mesmo nome em clusters diferentes. Cada sistema de storage com suporte do SnapCenter deve ter um nome exclusivo e um endereço IP de 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Faça backup de recursos SQL

Se um recurso ainda não fizer parte de qualquer grupo de recursos, você poderá fazer backup do recurso na página recursos.

Sobre esta tarefa

- Para autenticação de credenciais do Windows, você deve configurar sua credencial antes de instalar os plug-ins.
- Para autenticação de instância do SQL Server, você deve adicionar a credencial após a instalação dos plug-ins.
- Para autenticação gMSA, você deve configurar o gMSA enquanto Registra o host com o SnapCenter na página **Adicionar host** ou **Modificar host** para ativar e usar o gMSA.
- Se o host for adicionado com gMSA e se o gMSA tiver login e administrador do sistema Privileges, o gMSA poderá se conetar à instância 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 gMSA para ver se o plug-in SQL está operando atualmente. Se o plug-in estiver operando, ele será usado para estabelecer uma conexão com a instância SQL.
  - A instância SQL será acessada através da autenticação de credenciais do Windows quando a autenticação para instâncias SQL não estiver configurada e o plug-in não estiver operacional.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, selecione **Resources** e, em seguida, 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**.

   a. Selecione o banco de dados, instância ou grupo de disponibilidade que você deseja fazer backup.

      Quando você faz um backup de uma instância, as informações sobre o último status de backup ou o carimbo de data/hora dessa instância não estarão disponíveis na página recursos.

   Na visualização de topologia, não é possível diferenciar se o status do backup, o carimbo de data/hora ou o backup é para uma instância ou um banco de dados.

3. Na página recursos, marque a caixa de seleção **formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

   Por exemplo, customtext_policy_hostname ou resource_hostname. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

4. Na página políticas, execute as seguintes tarefas:

   a. Na seção políticas, selecione uma ou mais políticas na lista suspensa.

      Pode criar uma política selecionando + * * para iniciar o assistente de política.

      Na seção **Configurar programações para políticas selecionadas**, as políticas selecionadas são listadas.

   b. Selecione + * * na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

   c. Na caixa de diálogo **Adicionar programações para política** `policy_name`, configure a programação e selecione **OK**.

      ```
      `policy_name`Aqui está o nome da política que você selecionou.
      ```

   As programações configuradas são listadas na coluna **programações aplicadas**.

   a. Selecione o **Use o agendador do Microsoft SQL Server** e 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 está hospedando o banco de dados principal.

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 pretende configurar o seu agendamento de verificação e, em seguida, selecione * * + .

c. Na caixa de diálogo Adicionar agendas de verificação *policy_name*, execute as seguintes ações:

Se você quiser…	Faça isso…
Execute a verificação após a cópia de segurança	Selecione **Executar verificação após cópia de segurança**.
Marque uma verificação	Selecione **Executar verificação agendada**.

Se o servidor de verificação não tiver uma conexão de armazenamento, a operação de verificação falhará com erro: Falha ao montar o disco.

d. Selecione **OK**.

As programações configuradas são listadas na coluna agendas aplicadas.

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 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-SmtpServer.

7. Revise o resumo e selecione **Finish**.

A página de topologia do banco de dados é exibida.

8. Selecione **fazer uma cópia de segurança agora**.
9. Na página Backup, execute as seguintes etapas:

a. Se você tiver aplicado 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 **Verify after backup** para verificar o backup.

c. Selecione **Backup**.

Você não deve renomear a tarefa de backup criada no Windows Scheduler ou no SQL Server Agent.

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. Pode ver isto selecionando o respetivo utilizador ou grupo na página Acesso ao Utilizador. O tipo de grupo de recursos implícito é "recurso".

10. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Depois de terminar

- Nas configurações do MetroCluster, o SnapCenter pode não ser capaz de detetar uma relação de proteção após um failover.

  "Não é possível detetar a relação SnapMirror ou SnapVault após o failover do MetroCluster"

- Se você estiver fazendo backup de dados de aplicativos em VMDKs e o tamanho de heap Java para o plug-in SnapCenter para VMware vSphere não for grande o suficiente, o backup pode falhar. Para aumentar o tamanho do heap Java, localize o arquivo de script /opt/NetApp/init_scripts/scvservice. Nesse script, o `do_start method` comando inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: `Java -jar -Xmx8192M -Xms4096M`.

Informações relacionadas

"Criar políticas de backup para bancos de dados do SQL Server"

"Operações de backup falha com erro de conexão MySQL devido ao atraso no TCP_TIMEOUT"

"A cópia de segurança falha com o erro do programador do Windows"

"Operações de quiesce ou agrupamento de recursos falham"

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

   ```
   Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
   ```

   É apresentado o aviso de nome de utilizador e palavra-passe.

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 CrashConsistent:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Descubra os recursos do host usando o cmdlet Get-SmResources.

   Este exemplo descobre os recursos do 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. Exiba o status da tarefa de backup usando o cmdlet Get-SmBackupReport.

   Este exemplo exibe um relatório de resumo de todos os trabalhos 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*. Em alternativa, pode também consultar o "Guia de referência de 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 uma programação configurada, os backups ocorrerão automaticamente de acordo com a programação.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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. Em seguida, pode selecionar * * para fechar o painel do 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. Após o backup, selecione **Verify** para verificar o backup sob demanda.

      A opção **Verify** na política aplica-se apenas a trabalhos agendados.

   c. Selecione **Backup**.
5. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Informações relacionadas

"Criar políticas de backup para bancos de dados do SQL Server"

"Crie grupos de recursos e anexe políticas para o SQL Server"

"Operações de backup falha com erro de conexão MySQL devido ao atraso no TCP_TIMEOUT"

"A cópia de segurança falha com o erro do programador do Windows"

Monitore operações de backup de recursos SQL na página de tarefas do SnapCenter

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado correspondente das operações:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- 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 a que apenas as operações de cópia de segurança sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Backup**.
   d. Na lista suspensa **Status**, selecione o status da cópia de segurança.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.

   Embora o status do trabalho de backup seja exibido , quando você clica nos detalhes do trabalho, você pode ver que algumas das tarefas secundárias da operação de backup ainda estão em andamento ou marcadas com sinais de aviso.

5. Na página Detalhes da tarefa, clique em **Exibir logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Monitore operações de proteção de dados em recursos SQL no painel atividade

O painel atividade exibe as cinco operações mais recentes executadas. O painel atividade também é exibido quando a operação foi iniciada e o status da operação.

O painel atividade exibe informações sobre operações de backup, restauração, clone e backup agendadas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 da tarefa**.

Cancele o plug-in do SnapCenter para operações de backup do Microsoft SQL Server

Você pode cancelar operações de backup em execução, na fila ou sem resposta. Quando você cancela uma operação de backup, o servidor SnapCenter interrompe a operação e remove todos os snapshots do armazenamento se o backup criado não estiver registrado no servidor SnapCenter. Se o backup já estiver registrado no servidor SnapCenter, ele não reverterá o instantâneo já criado mesmo após o cancelamento ser acionado.

Antes de começar

- Você deve estar logado como administrador do SnapCenter ou proprietário da tarefa para cancelar as operações de restauração.
- Você pode cancelar apenas as operações de log ou backup completo que estão na fila ou em execução.
- Não é possível cancelar a operação após a verificação ter sido iniciada.

  Se cancelar a operação antes da verificação, a operação é cancelada e a operação de verificação não será executada.

- Pode cancelar uma operação de cópia de segurança a partir da página Monitor ou do painel atividade.
- Além de usar a GUI do SnapCenter, você pode usar cmdlets do PowerShell para cancelar operações.
- O botão **Cancelar trabalho** está desativado 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 em fila de outros membros enquanto usa essa função.

Passos

Execute uma das seguintes ações:

A partir do…	Ação
Página do monitor	1. No painel de navegação esquerdo, selecione **Monitor** > **trabalhos**. 2. Selecione o trabalho e selecione **Cancelar trabalho** .

A partir do…	Ação
Painel da atividade	1. Depois de iniciar o trabalho de cópia de segurança, selecione no painel atividade para ver 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 para o estado anterior. Se a operação cancelada não for responsiva no estado de cancelamento ou execução, você deverá executar `Cancel-SmJob -JobID <int> -Force` o cmdlet para interromper a operação de backup com força.

Veja os backups e clones do SQL Server na página topologia

Ao se preparar para fazer backup ou clonar um recurso, talvez seja útil exibir uma representação gráfica de todos os backups e clones no storage primário e secundário.

Sobre esta tarefa

Na página topologia, você pode ver todos os backups e clones disponíveis para o grupo de recursos ou recursos selecionado. Você pode visualizar os detalhes desses backups e clones e, em seguida, selecioná-los para executar operações de proteção de dados.

Você pode revisar os ícones a seguir na exibição **Gerenciar cópias** para determinar se os backups e clones estão disponíveis no storage primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups e clones disponíveis no storage primário.
- Exibe o número de backups e clones espelhados no storage secundário usando a tecnologia SnapMirror.
- Exibe o número de backups e clones replicados no storage secundário usando a tecnologia SnapVault.
  - O número de backups exibidos inclui os backups excluídos do armazenamento secundário.

    Por exemplo, se você criou backups 6 usando uma política para reter apenas 4 backups, o número de backups exibidos é 6.

> Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

Se você tiver uma relação secundária como sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), você poderá ver os seguintes ícones adicionais:

- O site da réplica está em cima.
- O site da réplica está inativo.
- A relação do espelho secundário ou do cofre não foi restabelecida.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o recurso ou o 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 é exibida.

4. Revise o cartão de resumo para ver um resumo do número de backups e clones disponíveis no storage primário e secundário.

   A seção **cartão de resumo** exibe o número total de backups e clones.

   Clicar no botão **Refresh** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clique no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Um horário semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo é espalhado por vários volumes, o tempo de expiração do SnapLock para o backup será o tempo de expiração do SnapLock mais longo definido para um snapshot em um volume. O tempo de expiração mais longo do SnapLock é recuperado do ONTAP.

   Para a 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 a relação de sincronização ativa do SnapMirror.

   - Para a sincronização ativa do SnapMirror e somente para o ONTAP 9.14,1, as relações de espelhamento do Async ou EspelrorVault do Async com o novo destino primário devem ser configuradas manualmente após o failover. A partir do ONTAP 9.15,1 em diante, o espelho do Async ou o MirrorVault do Async 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 **Refresh** somente depois que um backup tiver 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 um 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 estão no armazenamento secundário.

7. Selecione um clone da tabela e clique em **Clone Split**.
8. Se quiser excluir um clone, selecione-o na tabela e clique em .

Limpe a contagem de backup secundária usando cmdlets do PowerShell

Você pode usar o cmdlet Remove-SmBackup para limpar a contagem de backup para backups secundários que não têm Snapshot. Talvez você queira usar esse cmdlet quando o Total de snapshots exibido na topologia Gerenciar cópias não corresponder à configuração de retenção do Snapshot de storage 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 backup para backups secundários sem snapshots:

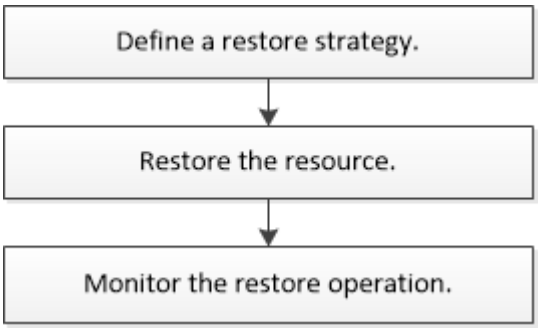
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Restaurar recursos do SQL Server

Restaure o fluxo de trabalho

Você pode usar o SnapCenter para restaurar bancos de dados 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 de banco de dados:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração, recuperação, verificação e clone. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte o. "Guia de referência de cmdlet do software SnapCenter"

Encontre mais informações

"Restaure um banco de dados SQL Server a partir do armazenamento secundário"

"Restaure e recupere 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 plug-in do SnapCenter para backup do Microsoft SQL Server, você deve garantir que vários requisitos sejam atendidos.

- A instância do SQL Server de destino deve estar on-line e em execução antes de poder restaurar um banco de dados.

  Isso se aplica às operações de restauração de banco de dados do usuário e às operações de restauração de banco de dados do sistema.

- As operações do SnapCenter que estão agendadas para serem executadas com base nos dados do SQL Server que você está restaurando devem ser desativadas, incluindo quaisquer tarefas agendadas em servidores de gerenciamento remoto ou verificação remota.
- Se os bancos de dados do sistema não estiverem funcionais, você deve primeiro reconstruir os bancos de dados do sistema usando um utilitário 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 de AG falha quando uma das seguintes condições for atendida:

  - Se o plug-in for instalado pelo usuário do RBAC e um administrador tentar restaurar um backup AG
  - Se o plug-in for instalado por um administrador e um usuário RBAC tentar restaurar um backup AG
- Se você estiver restaurando backups de diretório de log personalizados para um host alternativo, o servidor SnapCenter e o host do plug-in devem 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 banco de dados.
- Se você estiver replicando snapshots em um espelhamento ou cofre, o administrador do SnapCenter deverá ter atribuído as máquinas virtuais de storage (SVMs) para os volumes de origem e os volumes de destino.

  Para obter informações sobre como os administradores atribuem recursos aos usuários, consulte as informações de instalação do SnapCenter.

- Todos os trabalhos de cópia de segurança e clone têm de ser interrompidos antes de restaurar a base de dados.
- A operação de restauração pode ter tempo limite se o tamanho do banco de dados estiver em terabytes (TB).

  Você deve aumentar o valor do parâmetro RESTTimeout do servidor SnapCenter para 20000000 ms executando o seguinte comando: Set-SmConfigSettings -Agent -configSettings [20000000]. De acordo com o tamanho do banco de dados, o valor de tempo limite pode ser alterado e o valor máximo que você pode definir é de 86400000 ms.

Se você quiser restaurar enquanto os bancos de dados estiverem on-line, a opção de restauração on-line deve estar habilitada na página Restaurar.

Restaure backups de banco de dados do SQL Server

Você pode usar o SnapCenter para restaurar bancos de dados do SQL Server com backup. Restauração de 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 para 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 para um caminho alternativo, de modo que você não substitua uma versão de produção.

- O SnapCenter pode restaurar bancos de dados em um cluster do Windows sem colocar o grupo de cluster do SQL Server offline.
- Se ocorrer uma falha de cluster (uma operação de movimentação de grupo de cluster) durante uma operação de restauração (por exemplo, se o nó que possui os recursos for desativado), você deverá se reconetar à instância do SQL Server e reiniciar a operação de restauração.
- Não é possível restaurar o banco de dados quando os usuários ou as tarefas do SQL Server Agent estão acessando o banco de dados.
- Não é possível restaurar os bancos de dados do sistema para um caminho alternativo.
- O SCRIPT_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 usar o caminho padrão para segurança.

O valor da chave pode ser exibido do swagger através 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 Restaurar são auto-explicativos. As informações a seguir descrevem os campos para os quais você pode precisar de orientação.
- Para a operação de restauração de sincronização ativa do SnapMirror, você deve selecionar o backup no local principal.
- Para políticas habilitadas para o SnapLock, para ONTAP 9.12,1 e versões abaixo, se você especificar um período de bloqueio do Snapshot, os clones criados a partir dos snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

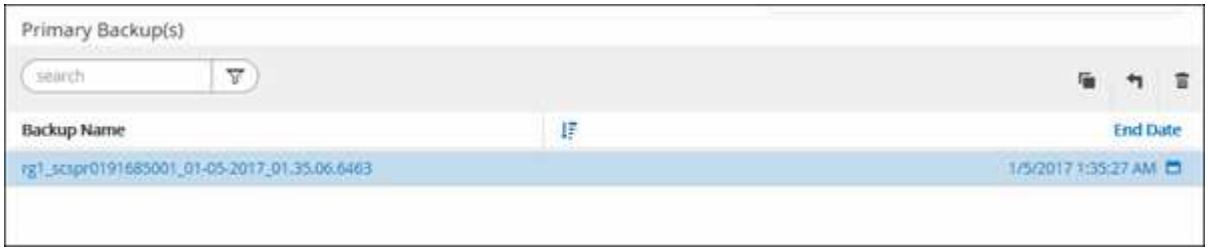
IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 a base de dados ou o grupo de recursos na lista.

   A página de topologia é exibida.

4. No modo de exibição Gerenciar cópias, selecione **backups** no sistema de armazenamento.
5. Selecione a cópia de segurança na tabela e, em seguida, clique no ícone.



6. Na página Restaurar escopo, selecione uma das seguintes opções:

Opção	Descrição
Restaure 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 em que os backups são feitos.
Restaure o banco de dados para um host alternativo	Selecione esta opção se quiser que o banco de dados seja restaurado para um servidor SQL diferente no mesmo ou em um host diferente no qual 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 igual à extensão de arquivo do arquivo de banco de dados original. Se a opção **Restaurar o banco de dados para um host alternativo** não for exibida na página Restaurar escopo, limpe o cache do navegador.

Opção	Descrição
Restaure o banco de dados usando arquivos de banco de dados existentes	Selecione esta opção se quiser que o banco de dados seja restaurado para um SQL Server alternativo no mesmo host ou diferente em que 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 âmbito de recuperação, selecione uma das seguintes opções:

Opção	Descrição
Nenhum	Selecione **nenhum** quando precisar restaurar somente o backup completo sem nenhum log.
Todos os backups de log	Selecione **todos os backups de log** operação de restauração de backup atualizada para restaurar todos os backups de log disponíveis após o backup completo.
Por backup de log até	Selecione **por backups de log** para executar uma operação de restauração pontual, que restaura o banco de dados com base em 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 transação não são 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
Use o diretório de log personalizado	Se tiver selecionado **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 para um host alternativo** ou **Restaurar o banco de dados usando os arquivos de banco de dados existentes**. Você também pode usar o caminho compartilhado, mas garantir que o caminho esteja acessível pelo usuário SQL. O diretório de log personalizado não é suportado para o 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 **reter configurações de replicação do banco de dados SQL** para restaurar o banco de dados e manter as configurações de replicação existentes.
      - Selecione **criar backup de log de transações antes de restaurar** para criar um log de transações antes do início da operação de restauração.
      - Selecione **Sair da restauração se o backup do log de transações antes da restauração falhar** para cancelar 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 prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

9. Na página Pós-operações, 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 transação adicionais** se você estiver restaurando todos os backups necessários agora.

        Esse é o comportamento padrão, que deixa o banco de dados pronto para uso, revertendo as transações não confirmadas. Não é possível restaurar registos de transações adicionais até

criar uma cópia de segurança.

- Selecione **não operacional, mas disponível para restaurar logs transacionais adicionais** para deixar o banco de dados não operacional sem reverter as transações não comprometidas.

  Logs de transação 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.

  Essa opção desfaz transações não confirmadas, mas salva as ações desfeitas em um arquivo de espera para que os efeitos de recuperação possam ser revertidos.

Se a opção Desfazer diretório estiver ativada, mais logs de transações serão restaurados. Se a operação de restauração do log de transações não for bem-sucedida, as alterações podem ser revertidas. A documentação do SQL Server contém mais informações.

b. Especifique scripts opcionais a serem executados após a execução de 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 prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_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 **Finish**.
12. Monitorize o processo de restauro utilizando a página **Monitor** > **trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 29th 2015 de janeiro a 3rd 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 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Restaure um banco de dados SQL Server a partir do armazenamento secundário

É possível restaurar os bancos de dados SQL Server com backup dos LUNs físicos (RDM, iSCSI ou FCP) em um sistema de storage 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 residente no sistema de storage secundário para um banco de dados especificado.

Antes de começar

- Você precisa ter replicado os snapshots do sistema de storage primário para o secundário.

- Você deve garantir que o servidor SnapCenter e o host do plug-in possam se conetar ao sistema de storage secundário.
- A maioria dos campos nas páginas do assistente de restauração são explicados no processo de restauração básico. As informações a seguir descrevem alguns dos campos para os quais você pode precisar de orientação.

Sobre esta tarefa

Para políticas habilitadas para o SnapLock, para ONTAP 9.12,1 e versões abaixo, se você especificar um período de bloqueio do Snapshot, os clones criados a partir dos snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

Passos

1. No painel de navegação à esquerda, clique em **Resources** 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 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** no sistema de armazenamento secundário (espelhado ou Vault).
5. Selecione a cópia de segurança 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 **Finish**.

Se você restaurou um banco de dados para um caminho diferente que é compartilhado por outros bancos de dados, você deve executar uma verificação completa de backup e backup para confirmar que seu banco de dados restaurado está livre de corrupção no nível físico.

Restaure recursos usando cmdlets do PowerShell

A restauração de um backup de recurso inclui iniciar uma sessão de conexão com o servidor SnapCenter, listar os backups e recuperar informações de backup e 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 servidor SnapCenter 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 29th 2015 de janeiro a 3rd 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 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Reseed Availability Group Databases

Reseed é uma opção para restaurar bancos de dados do Availability Group (AG). Se um banco de dados secundário ficar fora de sincronização com o banco de dados primário em um AG, você poderá fazer a semente novamente do banco de dados secundário.

Antes de começar

- Você deve ter criado o backup do banco de dados AG secundário que você deseja restaurar.
- O servidor SnapCenter e o host do plug-in devem ter a mesma versão do SnapCenter instalada.

Sobre esta tarefa

- Não é possível executar a operação de semente em bancos de dados primários.
- Não é possível executar uma operação de semente novamente se o banco de dados de réplica for removido do grupo de disponibilidade. Quando a réplica é removida, a operação de resemente falha.
- Ao executar a operação de repleed no banco de dados SQL Availability Group, você não deve acionar backups de log nos bancos de dados de réplica desse banco de dados de grupo de disponibilidade. Se você acionar backups de log durante a operação de repleed, a operação de repleed falha com o banco de dados espelhado, "database_name" tem dados de log de transação insuficientes para preservar a cadeia de backup de log da mensagem de erro principal do banco de dados.

Passos

1. No painel de navegação à esquerda, clique em **Resources** e selecione **SnapCenter Plug-in para SQL Server** na lista.
2. Na página recursos, selecione **Banco de dados** na lista **Exibir**.
3. Selecione a base de dados AG secundária na lista.
4. Clique em **Reseed**.
5. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Monitorar operações de restauração de recursos SQL

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um 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 executar.

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Restore**.

d. Na lista suspensa **Status**, selecione o status de restauração.

e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.

4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Cancelar operações de restauração de recursos SQL

Você pode cancelar trabalhos de restauração que estão na fila.

Você deve estar logado como administrador do SnapCenter ou proprietário da tarefa para cancelar as operações de restauração.

Sobre esta tarefa

- Você pode cancelar uma operação de restauração em fila na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de restauração em execução.
- Você pode usar a GUI do SnapCenter, cmdlets do PowerShell ou os comandos CLI para cancelar as operações de restauração em fila.
- O botão **Cancelar trabalho** está desativado para operações de restauração que não podem ser canceladas.
- Se você selecionou **todos os membros desta função podem ver e operar em outros objetos membros** na página usuários/grupos ao criar uma função, você pode cancelar as operações de restauração em fila de outros membros enquanto usa essa função.

Passo

Execute uma das seguintes ações:

A partir 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 da atividade	1. Depois de iniciar a operação de restauração, clique no painel atividade para exibir as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

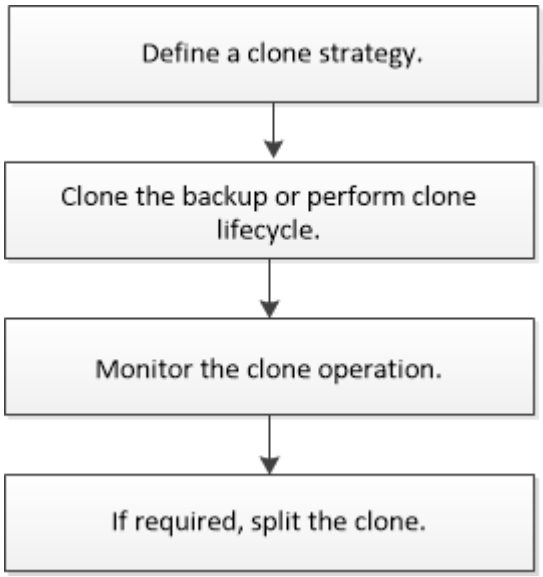
Clonar recursos de banco de dados do SQL Server

Fluxo de trabalho clone

É necessário executar várias tarefas usando o servidor SnapCenter antes de clonar os recursos do banco de dados a partir de um backup. 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 as ferramentas de extração e manipulação de dados ao preencher data warehouses ou para recuperar dados que foram excluídos ou alterados erroneamente.

Uma operação de clonagem de banco de dados gera relatórios com base nas IDs de tarefa.

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 clone. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte o. "Guia de referência de cmdlet do software SnapCenter"

Encontre mais informações

"Clone de um backup de banco de dados do SQL Server"

"Execute o ciclo de vida do clone"

"A operação de clone pode falhar ou levar mais tempo para ser concluída com o valor padrão TCP_TIMEOUT"

Clone de um backup de banco de dados do 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 bancos de dados sob demanda.

Antes de começar

- Você deve se preparar para a proteção de dados concluindo tarefas como adicionar hosts, identificar recursos e criar conexões do sistema de storage.
- Você deve ter feito backup de bancos de dados ou grupos de recursos.
- O tipo de proteção, como espelho, cofre ou espelho-Vault 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 de clone montada não puder ser encontrada durante uma operação de clone do SnapCenter, você deve alterar o parâmetro CloneRetryTimeout do servidor SnapCenter para 300.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de storage (SVM).

Sobre esta tarefa

- Durante a clonagem para uma instância de banco de dados autônoma, verifique se o caminho do ponto de montagem existe e se ele é um disco dedicado.
- Durante a clonagem para uma instância de cluster de failover (FCI), certifique-se de que os pontos de montagem existem, é um disco compartilhado e o caminho e o FCI devem pertencer ao mesmo grupo de recursos SQL.
- Verifique se há apenas um iniciador VFC ou FC conetado 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 SCRIPT_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 usar o caminho padrão para segurança.

  O valor da chave pode ser exibido do swagger através 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), verifique se o ponto de montagem é um disco dedicado.

- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

1. No painel de navegação à esquerda, selecione **Resources** 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 o grupo de recursos.
4. Na página de exibição **Gerenciar cópias**, selecione o backup do sistema de armazenamento primário ou secundário (espelhado ou abobadado).
5. Selecione a cópia de segurança e, em seguida, selecione *.
6. Na página **Clone Options**, execute as seguintes ações:

Para este campo…	Faça isso…
Servidor clone	Escolha um host no qual o clone deve ser criado.
Instância de clone	Escolha uma instância clone para a qual você deseja clonar o backup do banco de dados. Essa 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, forneça um sufixo para diferenciar o banco de dados clonado do banco de dados original. Caso contrário, a operação falha.
Atribuir automaticamente o ponto de montagem ou atribuir automaticamente o ponto de montagem do volume sob o caminho	Escolha se deseja atribuir automaticamente um ponto de montagem ou um ponto de montagem de volume sob um caminho. Atribuir automaticamente ponto de montagem de volume sob caminho: O ponto de montagem sob um caminho permite que você forneça um diretório específico. Os pontos de montagem serão criados dentro desse diretório. Antes de escolher essa 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.

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 quaisquer logs.
Todos os backups de log	Escolha esta opção para clonar todos os backups de log disponíveis datados após o backup completo.
Por backup 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 transação não são aplicados ao banco de dados clonado. Esse clone pontual interrompe o clone 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 prescritor ou postscript que devem ser executados antes ou depois da operação clone, respetivamente.

   Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.

   > O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

   O tempo limite padrão do script é de 60 segundos.

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 quiser anexar o relatório da operação clone executada, 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-SmtpServer.

   Para EMS, pode consultar "Gerir a recolha de dados EMS"

10. Revise o resumo e selecione **Finish**.
11. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Depois de terminar

Depois que o clone é criado, você nunca deve renomeá-lo.

Informações relacionadas

"A operação de clone pode falhar ou levar mais tempo para ser concluída com o valor padrão TCP_TIMEOUT"

"O clone do banco de dados de instância do cluster de failover falha"

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 clone a partir de um backup existente usando o cmdlet New-SmClone.

   Este exemplo cria um clone a partir 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. Exiba o status da tarefa clone usando o cmdlet Get-SmCloneReport.

   Este exemplo exibe um relatório de clone para a ID de tarefa especificada:

```
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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Execute o ciclo de vida do clone

Com o SnapCenter, você pode criar clones de um grupo de recursos ou banco de dados. Você pode executar um clone sob demanda ou agendar operações de clone 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 programe várias operações de clone para serem executadas simultaneamente em vários servidores.

Antes de começar

- Durante a clonagem para uma instância de banco de dados autônoma, verifique se o caminho do ponto de montagem existe e se ele é um disco dedicado.
- Durante a clonagem para uma instância de cluster de failover (FCI), certifique-se de que os pontos de montagem existem, é um disco compartilhado e o caminho e o FCI devem pertencer 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), verifique se o ponto de montagem é um disco dedicado.

Sobre esta tarefa

- O SCRIPT_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 usar o caminho padrão para segurança.

  O valor da chave pode ser exibido do swagger através 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 Clone Lifecycle são auto-explicativos. As informações a seguir descrevem os campos para os quais você pode precisar de orientação.
- Para a versão ONTAP 9.12,1 e inferior, 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 do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 **Clone Lifecycle**.
4. Na página Opções, execute as seguintes ações:

Para este campo…	Faça isso…
Clone o nome da tarefa	Especifique o nome da tarefa do ciclo de vida do clone que ajuda a monitorar e modificar a tarefa do ciclo de vida do clone.
Servidor clone	Escolha o host no qual o clone deve ser colocado.
Instância de clone	Escolha a instância clone para a qual você deseja clonar o banco de dados. Essa instância SQL deve estar localizada no servidor clone especificado.

Para este campo…	Faça isso…
Sufixo clone	Digite 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 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 "d.B1" de uma instância SQL "'inst1" e se "d.B1"" for clonado para "'inst1", então o nome do banco de dados clone deve ser "d.B1*clone".* *'"*clone" é um sufixo obrigatório definido pelo usuário porque o banco de dados é clonado para a mesma instância. Se "d.B1" for clonado para a instância SQL "'inst2", então o nome do banco de dados clone pode permanecer "d.B1" (o sufixo é opcional) porque o banco de dados é clonado para uma instância diferente.
Atribuir automaticamente o ponto de montagem ou atribuir automaticamente o ponto de montagem do volume sob o caminho	Escolha se deseja atribuir automaticamente um ponto de montagem ou um ponto de montagem de volume sob um caminho. Escolher atribuir automaticamente um ponto de montagem de volume sob um caminho permite fornecer um diretório específico. Os pontos de montagem serão criados dentro desse diretório. Antes de escolher essa 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 local, selecione um local de armazenamento para criar um clone.
6. Na página Script, insira o caminho e os argumentos do prescritor ou postscript que devem ser executados antes ou depois da operação clone, respetivamente.

   Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.

   > O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

   O tempo limite padrão do script é de 60 segundos.

7. Na página Agendar, execute uma das seguintes ações:
   - Selecione **Executar agora** se quiser executar a tarefa clone imediatamente.
   - Selecione **Configurar agendamento** quando quiser determinar com que frequência a operação de clone deve ocorrer, quando a programação de clones deve ser iniciada, em que dia a operação de clone deve ocorrer, quando a programação deve expirar e se os clones devem ser excluídos após a expiração da programação.
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 quiser anexar o relatório da operação clone executada, 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-SmtpServer.

Para EMS, pode consultar "Gerir a recolha de dados EMS"

9. Revise o resumo e clique em **Finish**.

Deve monitorizar o processo de clonagem utilizando a página **Monitor** > **trabalhos**.

Monitorar operações de clone de banco de dados SQL

Você pode monitorar o andamento das operações de clone do SnapCenter usando a página tarefas. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista para que apenas operações de clone sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Cancelar operações de clone de recursos SQL

Você pode cancelar as operações de clone que estão na fila.

Você deve estar logado como administrador do SnapCenter ou proprietário da tarefa para cancelar operações de clone.

Sobre esta tarefa

- Você pode cancelar uma operação de clone na fila a partir da página **Monitor** ou do painel **atividade**.
- Não é possível cancelar uma operação de clone em execução.
- Você pode usar a GUI do SnapCenter, cmdlets do PowerShell ou os comandos CLI para cancelar as operações de clone na fila.
- Se você selecionou **todos os membros desta função podem ver e operar em outros objetos membros** na página usuários/grupos enquanto cria uma função, você pode cancelar as operações de clone em fila de outros membros enquanto usa essa função.

Passo

Execute uma das seguintes ações:

A partir 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 da atividade	1. Depois de iniciar a operação clone, clique no painel atividade para exibir as cinco operações mais recentes. 2. Selecione a operação. 3. Na página **Detalhes do trabalho**, clique em **Cancelar trabalho**.

Divida um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido torna-se independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clones em um clone intermediário.

  Por exemplo, depois de criar clone1 a partir de um backup de banco de dados, você pode criar um backup de clone1 e clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e não é possível executar a operação de divisão de clones no clone1. No entanto, você pode executar a operação de divisão de clones no clone2.

  Depois de dividir clone2, você pode executar a operação de divisão de clones no clone1 porque clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e as tarefas de clone do clone são excluídas.
- Para obter informações sobre limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .

- Certifique-se de que o volume ou o agregado no sistema de storage esteja on-line.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página **recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicativos 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 do recurso é exibida.

4. No modo de 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 deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

   A operação de divisão de clones deixa de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clones e tentar novamente a operação de divisão de clones.

   Se você quiser um tempo de enquete mais longo 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 que o SMCore busque o status da operação de divisão de clones. O valor é em milissegundos e o valor padrão é de 5 minutos.

   Por exemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

   A operação de inicialização dividida de clone falhará se o backup, a restauração ou outra divisão de clones estiver em andamento. Você deve reiniciar a operação de divisão de clones somente depois que as operações em execução estiverem concluídas.

Informações relacionadas

"O clone ou a verificação do SnapCenter falha com o agregado não existe"

Proteger bancos de dados SAP HANA

Plug-in do SnapCenter para bancos de dados SAP HANA

Visão geral do plug-in do SnapCenter para banco de dados SAP HANA

O plug-in do SnapCenter para banco de dados SAP HANA é um componente do lado do host do software NetApp SnapCenter que permite o gerenciamento da proteção de dados com reconhecimento de aplicações 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 em seu ambiente SnapCenter.

O SnapCenter é compatível com contêineres únicos e contêineres de banco de dados multitenant (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 diferentes hosts.

Quando o plug-in para banco de dados SAP HANA é instalado, você pode 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 disco a disco para conformidade com os padrões.

O plug-in para banco de dados SAP HANA é compatível com a sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), que permite que os serviços empresariais continuem operando mesmo em caso de falha completa do local, dando suporte ao failover de aplicações de forma transparente usando uma cópia secundária. Nem a intervenção manual nem o script adicional são necessários para acionar um failover com a sincronização ativa do SnapMirror.

O que você pode fazer usando o plug-in do 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.
- Criar backups.
- Restauração a partir de backups.
- Backups de clones.
- Agendar operações de backup.
- Monitore operações de backup, restauração e clone.
- Exibir relatórios para operações de backup, restauração e clone.

Plug-in do SnapCenter para recursos de banco de dados SAP HANA

O SnapCenter se integra à aplicação plug-in e às tecnologias NetApp no sistema de storage. Para trabalhar com o plug-in para banco de dados SAP HANA, você usa a

interface gráfica do usuário do SnapCenter.

- * Interface gráfica unificada do usuário*

  A interface do SnapCenter fornece padronização e consistência em plug-ins e ambientes. A interface do SnapCenter permite concluir operações consistentes de backup, restauração e clone em plug-ins, usar relatórios centralizados, usar visualizações de painel rápidas, configurar controle de acesso baseado em funções (RBAC) e monitorar tarefas em todos os plug-ins.

- * Administração central automatizada*

  Você pode agendar operações de backup, configurar a retenção de backup baseada em política e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- **Tecnologia de cópia Snapshot NetApp sem interrupções**

  A 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 a fluxos de trabalho de backup, restauração e clone
- Delegação de funções centralizada e segurança compatível com RBAC

  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 uso eficiente de espaço e pontuais para teste ou extração de dados usando a tecnologia NetApp FlexClone

  É necessária uma licença FlexClone no sistema de storage onde você deseja criar o clone.

- Suporte ao recurso Snapshot do grupo de consistência (CG) do ONTAP como parte da criação de backups.
- Funcionalidade de executar vários backups simultaneamente em vários hosts de recursos

  Em uma única operação, os snapshots são consolidados quando os recursos em um único host compartilham o mesmo volume.

- Capacidade de criar instantâneos usando comandos externos.
- Suporte para backup baseado em arquivos.
- Suporte para Linux LVM no sistema de arquivos XFS.

Tipos de storage compatíveis com o 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 máquinas virtuais (VMs). Você deve verificar o suporte para seu tipo de storage antes de instalar o plug-in SnapCenter para banco de dados SAP HANA.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados a FC • LUNs ligados ao iSCSI • Volumes conectados a NFS
VMware ESXi	• LUNs RDM conetados por um FC ou iSCSI ESXi HAScanning de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluído 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** para 1 para reexaminar somente os HBA listados em HBA_DRIVER_NAMES. • ISCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI • VMDKs em armazenamentos de dados NFS • VMDKs no VMFS criado • Volumes NFS conectados diretamente ao sistema convidado • Armazenamentos de dados da VVol em NFS e SAN O armazenamento de dados da VVol só pode ser provisionado com as Ferramentas do ONTAP para o VMware vSphere.

Mínimo de ONTAP Privileges necessário para plug-in SAP HANA

Os ONTAP Privileges mínimos necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
  - event generate-AutoSupport-log
  - mostra o histórico de trabalhos
  - paragem do trabalho
  - lun
  - lun criar
  - lun criar

- lun criar
- eliminação lun
- lun igrop add
- lun igrop criar
- eliminação do agrupamento lun
- mudar o nome do grupo lun
- mudar o nome do grupo lun
- show de grupos de lun
- nós complementares de mapeamento de lun
- mapeamento lun criar
- eliminação do mapeamento lun
- mapeamento lun remove-reporting-nonos
- mostra de mapeamento lun
- modificação de lun
- movimentação de lun no volume
- lun offline
- lun online
- limpeza da reserva persistente de lun
- redimensionar lun
- série lun
- mostra lun
- regra adicional de política do SnapMirror
- regra de modificação de política do SnapMirror
- regra de remoção da política do SnapMirror
- SnapMirror policy show
- restauração de SnapMirror
- SnapMirror show
- SnapMirror show-history
- atualização do SnapMirror
- SnapMirror update-ls-set
- SnapMirror lista-destinos
- versão
- clone de volume criar
- show de clone de volume
- início da divisão do clone de volume
- paragem dividida clone volume
- criar volume

    - destruição de volume
    - clone de arquivo de volume criar
    - show-disk-use do arquivo de volume
    - volume off-line
    - volume online
    - modificação do volume
    - criar qtree de volume
    - eliminação de qtree de volume
    - modificação de qtree de volume
    - apresentação de qtree de volume
    - restrição de volume
    - apresentação do volume
    - criar instantâneo de volume
    - eliminar instantâneo do volume
    - modificação do instantâneo do volume
    - tempo de expiração do volume snapshot modify-SnapLock
    - mudar o nome do instantâneo do volume
    - restauração de snapshot de volume
    - restauração de arquivo de snapshot de volume
    - apresentação de instantâneo do volume
    - desmontar o volume
    - svm cifs
    - compartilhamento cifs de svm criar
    - exclusão de compartilhamento cifs de svm
    - apresentação do shadowcopy cifs de svm
    - exibição de compartilhamento cifs de svm
    - mostra cifs de svm
    - política de exportação de svm
    - criação de política de exportação de svm
    - exclusão da política de exportação do svm
    - regra de política de exportação de svm criar
    - a regra de política de exportação do svm é exibida
    - exibição da política de exportação do svm
    - svm iscsi
    - apresentação da ligação iscsi de svm
    - mostra o svm
- Comandos somente leitura: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior

- interface de rede
- mostra da interface de rede
- svm

Preparar sistemas de storage para replicação do SnapMirror e do SnapVault para bancos de dados SAP HANA

Você pode usar um plug-in do 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 disco a disco para conformidade com os padrões e outros fins relacionados à governança. Antes de executar essas tarefas, você deve configurar uma relação de proteção de dados entre os volumes de origem e destino e inicializar a relação.

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 . Se você estiver usando a sincronização ativa do SnapMirror , use os agendamentos padrão do SnapMirror ou SnapVault para a sincronização ativa do SnapMirror e para relacionamentos assíncronos.

Se você estiver vindo para o SnapCenter de um produto NetApp SnapManager e estiver satisfeito com as relações de proteção de dados que configurou, ignore esta seção.

Uma relação de proteção de dados replica dados no storage primário (o volume de origem) para o storage secundário (o volume de destino). Ao inicializar a relação, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não suporta relações em cascata entre volumes SnapMirror e SnapVault (**Primary** > **Mirror** > **Vault**). Você deve usar relacionamentos de fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis 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 seus trabalhos de backup ajuda a ter os backups necessários para restaurar ou clonar seus recursos com êxito. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (rto) e objetivo do ponto de restauração (RPO) determinam em grande parte a sua estratégia de backup.

Sobre esta tarefa

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. Rto é o momento em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a era dos arquivos que precisam 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 de seus recursos.
2. Decida quantos trabalhos de cópia de segurança necessita.
3. Decida como nomear seus backups.
4. Decida se você deseja criar uma política baseada em cópia Snapshot para fazer backup de snapshots consistentes com aplicações do banco de dados.
5. Decida se 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 a longo prazo.
7. Determine o período de retenção dos snapshots no sistema de storage de origem e no destino do SnapMirror.
8. Determine se deseja executar quaisquer comandos antes ou depois da operação de backup e forneça um prescritor ou postscript.

Descoberta automática de recursos no host Linux

Os recursos são bancos de dados SAP HANA e volume não-dados no host Linux gerenciado pelo SnapCenter. Depois de instalar o plug-in do SnapCenter para o banco de dados SAP HANA, os bancos de dados SAP HANA nesse host Linux são automaticamente descobertos e exibidos na página recursos.

A detecção automática é compatível com os seguintes recursos do SAP HANA:

- Contêineres únicos

  Depois de instalar ou atualizar o plug-in, os recursos de contentor único localizados em um plug-in de host centralizado continuarão como recursos adicionados manualmente.

  Depois de instalar ou atualizar o plug-in, os bancos de dados SAP HANA são automaticamente descobertos apenas nos hosts do SAP HANA Linux, que são registrados diretamente no SnapCenter.

- Contêiner de banco de dados multitenant (MDC)

  Depois de instalar ou atualizar o plug-in, os recursos do MDC localizados em um plug-in de host centralizado continuarão como recurso adicionado manualmente.

  Você deve continuar a adicionar manualmente os recursos do MDC no plug-in de host centralizado após a atualização para o SnapCenter 4,3.

  Para hosts SAP HANA Linux diretamente registrados no SnapCenter, a instalação ou atualização do plug-in acionará uma descoberta automática de recursos no host. Depois de atualizar o plug-in, para cada recurso MDC que estava localizado no host do plug-in, outro recurso MDC será automaticamente descoberto com um formato GUID diferente e registrado no SnapCenter. O novo recurso estará no 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 deteção 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 são suportadas por esses recursos.

- Configuração de vários host HANA
- Várias instâncias no mesmo host
- Replicação do SISTEMA HANA com escalabilidade horizontal de várias camadas
- Ambiente de replicação em cascata no modo de replicação do sistema

Tipos de backups suportados

Tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter é compatível com os tipos de backup baseado em cópia de Snapshot e backup baseado em arquivos para bancos de dados SAP HANA.

Backup baseado em arquivo

Os backups baseados em arquivos verificam a integridade do banco de dados. Você pode agendar a operação de backup baseada em arquivo para ocorrer em intervalos específicos. Somente os locatários ativos são copiados. Não é possível restaurar e clonar backups baseados em arquivos do SnapCenter.

Backup baseado em cópia snapshot

Os backups baseados em cópias snapshot utilizam a tecnologia NetApp Snapshot para criar cópias on-line e somente leitura dos volumes nos quais os bancos de dados SAP HANA estão localizados.

Como o plug-in do SnapCenter para banco de dados SAP HANA usa snapshots de grupo de consistência

Você pode usar o plug-in para criar instantâneos de grupo de consistência para grupos de recursos. Um grupo de consistência é um contentor que pode abrigar vários volumes para que você possa gerenciá-los como uma entidade. Um grupo de consistência é snapshots 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 **descontraído**. Você também pode ativar ou desativar a sincronização WAFL (Write Anywhere File Layout) durante a operação de captura instantânea de grupo consistente. O WAFL Sync melhora o desempenho de um grupo de consistência instantâneo.

Como o SnapCenter gerencia o gerenciamento de backups de log e dados

O SnapCenter gerencia o serviço de limpeza dos backups de log e dados nos níveis do sistema de storage e do sistema de arquivos e no catálogo de backup do SAP HANA.

Os snapshots no storage primário ou secundário e suas entradas correspondentes no catálogo do SAP HANA são excluídos com base nas configurações de retenção. As entradas do catálogo do SAP HANA também são excluídas durante a exclusão do grupo de recursos e backup.

Considerações para determinar programações de backup para banco de dados SAP HANA

O fator mais crítico na determinação de um agendamento de backup é a taxa de alteração do recurso. Você pode fazer backup de um recurso muito usado a cada hora, enquanto você pode fazer backup de um recurso raramente usado uma vez por dia. Outros fatores incluem a importância do recurso para a sua organização, seu contrato de nível de serviço (SLA) e seu objetivo do ponto de restauração (RPO).

Os programas de backup têm duas partes, como segue:

- Frequência de backup (com que frequência os backups devem ser executados)

  A frequência de backup, também chamada de tipo de programação para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como hora, dia, semanal ou mensal.

- Programações de backup (exatamente quando os backups devem ser executados

  As agendas de backup fazem parte de uma configuração de recurso ou grupo de recursos. Por exemplo, se você tiver um grupo de recursos que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas

Número de tarefas de backup necessárias para bancos de dados SAP HANA

Os fatores que determinam o número de tarefas de backup de que você precisa 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 padrão de nomenclatura Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um carimbo de data/hora aos nomes de Snapshot 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 carimbo de data/hora.

Como alternativa, você pode especificar o formato do nome da captura Instantânea enquanto protege recursos ou grupos de recursos selecionando **usar formato de nome personalizado para cópia Instantânea**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do carimbo de hora é adicionado ao nome do instantâneo.

Estratégia de restauração e recuperação para bancos de dados SAP HANA

Definir uma estratégia de restauração e recuperação para recursos do SAP HANA

Você deve definir uma estratégia antes de restaurar e recuperar seu banco de dados para que você possa executar operações de restauração e recuperação com sucesso.

Passos

1. Determine as estratégias de restauração com suporte para recursos do SAP HANA adicionados manualmente
2. Determinar as estratégias de restauração com suporte 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 compatíveis com recursos do SAP HANA adicionados manualmente

Você deve definir uma estratégia antes de executar operações de restauração com êxito usando o SnapCenter. Existem dois tipos de estratégias de restauração para recursos do 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 instantâneos obtidos 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.

Restauração no nível do arquivo

- Restaura arquivos de volumes, qtrees ou diretórios
- Restaura apenas os LUNs selecionados

Tipos de estratégias de restauração compatíveis com bancos de dados SAP HANA descobertos automaticamente

Você deve definir uma estratégia antes de executar operações de restauração com êxito usando o SnapCenter. Existem 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 todo o volume.

> Se o recurso contiver volumes ou qtrees, os instantâneos obtidos 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.

Banco de dados de inquilinos

- Restaura o banco de dados do locatário

Se a opção **Banco de dados do locatário** estiver selecionada, os scripts de recuperação HANA ou HANA externos ao SnapCenter devem ser usados para executar a operação de recuperação.

Tipos de operações de restauração para bancos de dados SAP HANA descobertos automaticamente

O SnapCenter é compatível com SnapRestore baseado em volume (VBSR), SnapRestore de arquivo único e tipos de restauração de conexão e cópia 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 é 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 **Reverter volume** estiver selecionada

O SnapRestore de arquivo único 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** estiver selecionada
- Para contentores de banco de dados multitenant (MDC), quando o backup selecionado para restauração é feito no SnapCenter 4,3 e a opção **Banco de dados do locatário** está selecionada
- Quando o backup selecionado é de um local secundário SnapMirror ou SnapVault e a opção **recurso completo** está selecionada

O SnapRestore de Arquivo único 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 em um local secundário do SnapMirror ou do SnapVault e a opção **recurso completo** está selecionada

A restauração baseada em conexão e cópia é realizada 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 do locatário** é selecionada

> **As opções recurso completo**, **Reverter volume** e **Banco de dados do locatário** estão disponíveis na página Restaurar escopo.

Tipos de operações de recuperação compatíveis com bancos de dados SAP HANA

O SnapCenter permite que você execute diferentes tipos de operações de recuperação para bancos de dados SAP HANA.

- Recupere o banco de dados até o estado mais recente
- Recupere o banco de dados até um ponto específico no tempo

  Você deve especificar a data e a hora para a recuperação.

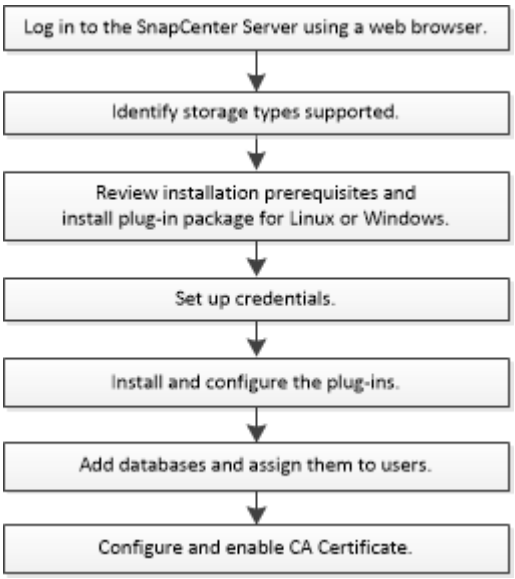
- Recupere o banco de dados até um backup de dados específico

O SnapCenter também fornece a opção sem recuperação para bancos de dados SAP HANA.

Prepare-se para instalar o plug-in do SnapCenter para o 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 plug-in do SnapCenter para o banco de dados SAP HANA se quiser proteger os bancos de dados SAP HANA.



Pré-requisitos para adicionar hosts e instalar o plug-in do SnapCenter para banco de dados SAP HANA

Antes de adicionar um host e instalar os pacotes de plug-in, você deve completar todos os requisitos. O plug-in do SnapCenter para banco de dados SAP HANA está disponível em ambientes Windows e Linux.

- Você deve ter instalado o Java 11 em seu host.

  O IBM Java não é suportado.

- Você deve ter instalado o terminal interativo do banco de dados SAP HANA (cliente HDBSQL) no host.
- Para o Windows, o Plug-in Creator Service deve ser executado usando o usuário Windows '"LocalSystem"', que é o comportamento padrão quando o Plug-in para SAP HANA Database é instalado como administrador de domínio.
- Para o Windows, as chaves de armazenamento de usuários devem ser criadas como usuário DO SISTEMA.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host. O plug-in do SnapCenter para Microsoft Windows será implantado por padrão com o plug-in SAP HANA em hosts do Windows.
- Para o host Linux, as chaves HDB Secure User Store são acessadas como usuário HDBSQL os.
- O servidor SnapCenter deve ter acesso ao 8145 ou à porta personalizada do plug-in para o host de banco de dados SAP HANA.

Hosts do Windows

- Você deve ter um usuário de domínio com Privileges de administrador local com permissões de login local no host remoto.
- Ao instalar o plug-in para banco de dados SAP HANA em um host Windows, o plug-in do SnapCenter 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 em seu host Windows.

  "Downloads Java para todos os sistemas operacionais"

  "Ferramenta de Matriz de interoperabilidade do 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 em seu host Linux.

  "Downloads Java para todos os sistemas operacionais"

  "Ferramenta de Matriz de interoperabilidade do NetApp"

- Para bancos de dados SAP HANA que estão sendo executados em um host Linux, ao instalar o plug-in para banco de dados SAP HANA, o plug-in do SnapCenter para UNIX é instalado automaticamente.

- Você deve ter **bash** como o shell padrão para instalação do plug-in.

Comandos suplementares

Para executar um comando complementar no plug-in do SnapCenter para SAP HANA, você deve incluí-lo no arquivo *allowed_commands.config*.

- Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
- Localização 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 são sensíveis a maiúsculas e minúsculas. Certifique-se de especificar o nome de caminho totalmente qualificado e incluir o nome de caminho entre aspas (") se ele contiver espaços.

Por exemplo:

comando: montar

comando: umount

Comando: "C: Arquivos de programas/comandos NetApp/sdcli.exe"

comando: myscript.bat

Se o arquivo *allowed_commands.config* não estiver presente, os comandos ou a execução de 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.

Configure sudo Privileges 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 de plug-in serão executados como um usuário não-root eficaz. Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se o umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro devem ter permissão de 555. Caso contrário, a instalação do plug-in pode falhar.
- Para o usuário não-root, certifique-se de que o nome do usuário não-root e do grupo do usuário devem ser os mesmos.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos de código de autenticação de

mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

Reinicie o serviço sshd depois de 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 o sudo Privileges para que o usuário não-root forneça acesso aos seguintes caminhos:

- /Home/*Linux_USER*/.SC_NetApp/SnapCenter_linux_host_plugin.bin
- /Custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/SnapCenter/spl/bin/spl

Passos

1. Faça 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 !visiblepw
Defaults: LINUX_USER !requiretty
```

Se você estiver tendo uma configuração RAC, juntamente 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**, que está localizado em:

- Se o servidor SnapCenter estiver instalado no host do Windows, o SnapCenter NetApp não será instalado no sistema operacional Windows.
- */opt/NetApp/SnapCenter/SnapManagerWeb/Repository/SC_UNIX_plugins_checksum.txt* se o servidor SnapCenter 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 do 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 do sistema host e requisitos de dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• .NET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet."

Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux

Antes de instalar o pacote de plug-ins do 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 • SUSE Linux Enterprise Server (SLES) Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto. Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do 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 raiz ou para um usuário não-root que tenha sudo Privileges para instalar e iniciar o processo de plug-in.

Prática recomendada: embora você tenha permissão para criar credenciais para Linux após implantar hosts e instalar plug-ins, a prática recomendada é criar credenciais após adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

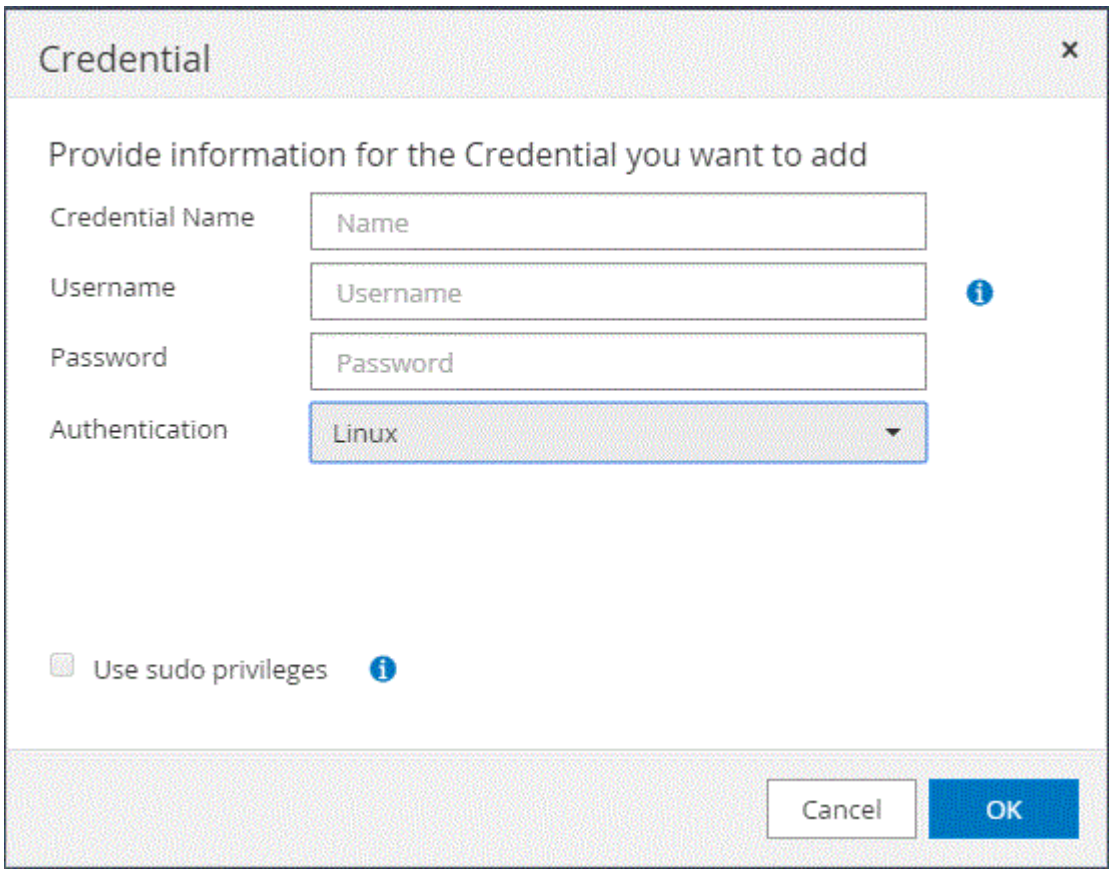
  Você deve configurar as credenciais do Windows antes de instalar os plug-ins.

  Você deve configurar as credenciais com o Privileges 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 Privileges de administrador completo, será necessário atribuir pelo menos o grupo de recursos e Privileges de backup ao nome de usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Clique em **novo**.



4. Na página Credential (credencial), especifique as informações necessárias para configurar credenciais:

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para as credenciais.
Nome de utilizador	Introduza o nome de utilizador e a palavra-passe a utilizar para a 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 no qual você está instalando o plug-in do SnapCenter. Formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS_username* ◦ *Domain FQDN_username* • Administrador local (apenas para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é: *Nome de usuário* Não use aspas duplas (") ou backtick (') nas senhas. Você não deve usar os símbolos menos de (>) e exclamação (!) juntos em senhas. Por exemplo, lessthan!10, lessthan10You!, backtick'12.
Palavra-passe	Introduza a palavra-passe utilizada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que pretende utilizar.
Use sudo Privileges	Marque a caixa de seleção **Use sudo Privileges** se estiver criando credenciais para um usuário que não seja root. Aplicável apenas a usuários 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.

Configure o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite criar uma conta de serviço gerenciado de grupo (gMSA) que fornece gerenciamento automatizado de senha de conta de serviço a partir de uma conta de domínio gerenciado.

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 é um membro do domínio.

Passos

1. Crie uma chave raiz KDS para gerar senhas exclusivas para cada objeto em seu gMSA.
2. Para cada domínio, execute o seguinte comando do 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,…>
.. Execute `Get-ADServiceAccount` o comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Ative o módulo do ative Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando do 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 o host.

b. Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua o Privileges administrativo ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no servidor SnapCenter.

   O servidor SnapCenter 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 do SnapCenter para bancos de dados SAP HANA

Adicione hosts e instale pacotes plug-in 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 servidor SnapCenter for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deve executar o seguinte:
  - Atualize para o Windows Server 2019 (versão de SO 17763,5936) ou posterior
  - Atualize para o Windows Server 2022 (versão de SO 20348,2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está

integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar 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 você estiver usando a conta de serviço gerenciado de grupo (gMSA), você deve configurar o gMSA com Privileges administrativo.

  "Configurar conta de serviço gerenciado de grupo no Windows Server 2016 ou posterior para SAP HANA"

Sobre esta tarefa

- Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.
- Para que a replicação do sistema SAP HANA descubra recursos em sistemas primários e secundários, recomenda-se adicionar os sistemas primário e secundário usando o usuário raiz ou sudo.

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Verifique se a guia **hosts gerenciados** está selecionada na parte superior.
3. Clique em **Add**.
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 cliente HDBSQL, e esse host pode estar em um sistema Windows ou em um sistema Linux.
Nome do host	Insira o nome do host de comunicação. Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no 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 exibir detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você forneceu. 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 instalar.
6. (Opcional) clique em **mais opções**.

Para este campo…	Faça isso…
Porta	Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido 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, você deve especificar a mesma porta. Caso contrário, a operação falha.
Caminho de instalação	O plug-in para SAP HANA é instalado no host cliente HDBSQL, e esse host pode estar em um sistema Windows ou em um sistema Linux. • Para o pacote de plug-ins do 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 do SnapCenter para Linux, o caminho padrão é /opt/NetApp/SnapCenter. Opcionalmente, você pode personalizar o caminho.

Para este campo…	Faça isso…
Ignorar as verificações de pré-instalação	Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	Para o host Windows, marque essa caixa de seleção se desejar usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in. Forneça o nome do gMSA no seguinte formato: O gMSA será usado como uma conta de serviço de logon apenas para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

   Se você não tiver selecionado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se o host 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 Java (para plug-ins do Linux) são validados de acordo com os requisitos mínimos. Se os requisitos mínimos não forem cumpridos, são apresentadas mensagens de erro ou de aviso adequadas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado no NetApp SnapCenter para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, será necessário atualizar o arquivo em ambos os nós.

8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirm and Submit**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós no cluster.

   A verificação de impressões digitais é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitorize o progresso da instalação.

   Os arquivos de log específicos da instalação estão localizados em /custom_location/SnapCenter/logs.

Instale pacotes de plug-ins do 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 PowerShell.

Antes de começar

Você deve ter feito 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 servidor SnapCenter, 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*. Em alternativa, pode também consultar o "Guia de referência de 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 do SnapCenter para o banco de dados SAP HANA em hosts Linux usando a interface de linha de comando

Você deve instalar o plug-in do SnapCenter para banco de dados SAP HANA usando a interface de usuário (UI) do SnapCenter. Se o seu ambiente não permitir a instalação remota do plug-in a partir da IU do SnapCenter, você pode instalar o plug-in para banco de dados SAP HANA no modo 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 reside o cliente HDBSQL.
- O host Linux no qual você está instalando o plug-in do SnapCenter para 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 do SnapCenter para banco de dados SAP HANA faz parte do pacote de plug-ins do SnapCenter para Linux. Antes de instalar o pacote de plug-ins do SnapCenter para Linux, você já deve ter instalado o SnapCenter em um host do Windows.

Passos

1. Copie o pacote de plug-ins do SnapCenter para o arquivo de instalação do Linux (SnapCenter_linux_host_plugin.bin) do repositório C:/NetApp/SnapCenter 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 servidor SnapCenter 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 SMCore.
   - -DSERVER_IP especifica o endereço IP do servidor SnapCenter.
   - -DSERVER_HTTPS_PORT especifica a porta HTTPS do servidor SnapCenter.
   - -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 /<installation directory>/NetApp/SnapCenter/scc/etc/SC_SMS_Services.properties e, em seguida, adicione o parâmetro PLUGINS_ENABLED: HANA:3,0.
5. Adicione o host ao servidor SnapCenter 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Monitore o status da instalação do plug-in para SAP HANA

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, para filtrar a lista de modo a que apenas as operações de instalação de plug-in

sejam listadas, faça o seguinte:

a. Clique em **filtro**.
b. Opcional: Especifique a data de início e fim.
c. No menu suspenso tipo, selecione **Instalação 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 **Visualizar logs**.

Configurar certificado CA

Gerar arquivo CSR do 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 a CSR gerada. O certificado terá uma chave privada associada a ele.

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

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

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

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

Para configurações de cluster, o nome do cluster (FQDN de cluster virtual) e os respetivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome alternativo (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados CA

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 **Yes**, importe a chave privada e clique em **Next**.
Importar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

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

7. Repita o passo 5 para a pasta "Pessoal".

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia 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 **thumbprint**.
   d. Copie os carateres 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

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.

Configure o certificado CA com os serviços de plug-in do host do Windows

Você deve configurar o certificado CA com os serviços de plug-in host do Windows para

ativar o certificado digital instalado.

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, 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"
   ```

Configure o certificado de CA para o serviço de plug-ins SAP HANA do SnapCenter 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. Altere a senha do keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Altere a senha para 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 depois de 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. Liste 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 de CA raiz e, em seguida, os certificados de CA intermediários.

Configurar o par de chaves assinadas pela CA para plug-in de armazenamento confiável

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. Liste 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. Liste os certificados adicionados no keystore.

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

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

   A senha padrão do keystore 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 espaço ou
carateres 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 com a chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o plug-in trust-store.

Configurar a lista de revogação de certificados (CRL) para plug-ins do SnapCenter

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 SnapCenter é 'opt/NetApp/snapcenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties contra a chave CRL_PATH.

   Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Configure o certificado de CA para o serviço de plug-ins SAP HANA do SnapCenter no host do 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 Plug-ins 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. Altere 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 por seu caminho completo.

   C: Arquivos de programas/<jdk_version>/keytool.exe" -storepasswd -keystore keystore.jks

3. Altere a senha para 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*.

4. Reinicie o serviço depois de 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. Liste 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 de CA raiz e, em seguida, os certificados de CA intermediários.

Configurar o par de chaves assinadas pela CA para plug-in de armazenamento confiável

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. Liste 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 -destinkeystore keystore.jks -deststoretype JKS

5. Liste os certificados adicionados no keystore.

   keytool -list -v -keystore keystore.jks

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da 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

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

   Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o plug-in trust-store.

Configurar a lista de revogação de certificados (CRL) para plug-ins do SnapCenter

Sobre esta tarefa

- Para transferir o ficheiro CRL mais recente para o certificado CA relacionado, "Como atualizar o arquivo de lista de revogação de certificados no certificado da CA do SnapCenter"consulte .
- 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* contra a chave CRL_PATH.

2. Você pode colocar mais de um arquivo CRL neste diretório.

   Os certificados recebidos serão verificados em relação a cada CRL.

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet RUN *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando as *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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- * * Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da 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 são concluídas com êxito.

Instale o plug-in do SnapCenter para VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs) ou se você quiser proteger VMs e datastores, você deverá implantar o plug-in do SnapCenter para o dispositivo virtual VMware vSphere.

Para obter informações sobre como implantar, "Visão geral da implantação" consulte .

Implantar certificado CA

Para configurar o certificado CA com o plug-in SnapCenter para VMware vSphere, "Criar ou importar certificado SSL" consulte .

Configure o arquivo CRL

O plug-in do SnapCenter para VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL para o plug-in do SnapCenter para 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.

Preparar-se para a proteção de dados

Pré-requisitos para usar o plug-in do SnapCenter para banco de dados SAP HANA

Antes de usar o plug-in do SnapCenter para banco de dados SAP HANA, o administrador do SnapCenter deve instalar e configurar o servidor SnapCenter e executar as tarefas de pré-requisito.

- Instalar e configurar o servidor SnapCenter.
- Inicie sessão no servidor SnapCenter.
- Configure o ambiente SnapCenter adicionando conexões do sistema de storage e criando credenciais, se aplicável.
- Instale o Java 11 em seu host Linux ou Windows.

  Você deve definir o caminho Java na variável caminho ambiental da máquina host.

- Configure o SnapMirror e o SnapVault, se quiser 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 do armazenamento de usuários para os nós do SAP HANA que você gerenciará por meio desse host.

- Para o banco de dados SAP HANA 2.0SPS05, se você estiver usando uma conta de usuário do banco de dados SAP HANA, verifique se você tem as seguintes permissões para executar operações de backup, restauração e clone no servidor SnapCenter:
  - Administrador de backup
  - Catálogo lido
  - Administrador de backup de banco de dados
  - Operador de recuperação de banco de dados

Como os recursos, grupos de recursos e políticas são usados para proteger bancos de dados do SAP HANA

Antes de usar o SnapCenter, é útil entender 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 clonar com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host.

  Quando você executa uma operação em um grupo de recursos, executa essa operação nos recursos definidos no grupo de recursos de acordo com a programação especificada 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 programados para recursos únicos e grupos de recursos.

- As políticas especificam a frequência do backup, a replicação, os scripts e outras caraterísticas 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 quando você executa um backup sob demanda para um único recurso.

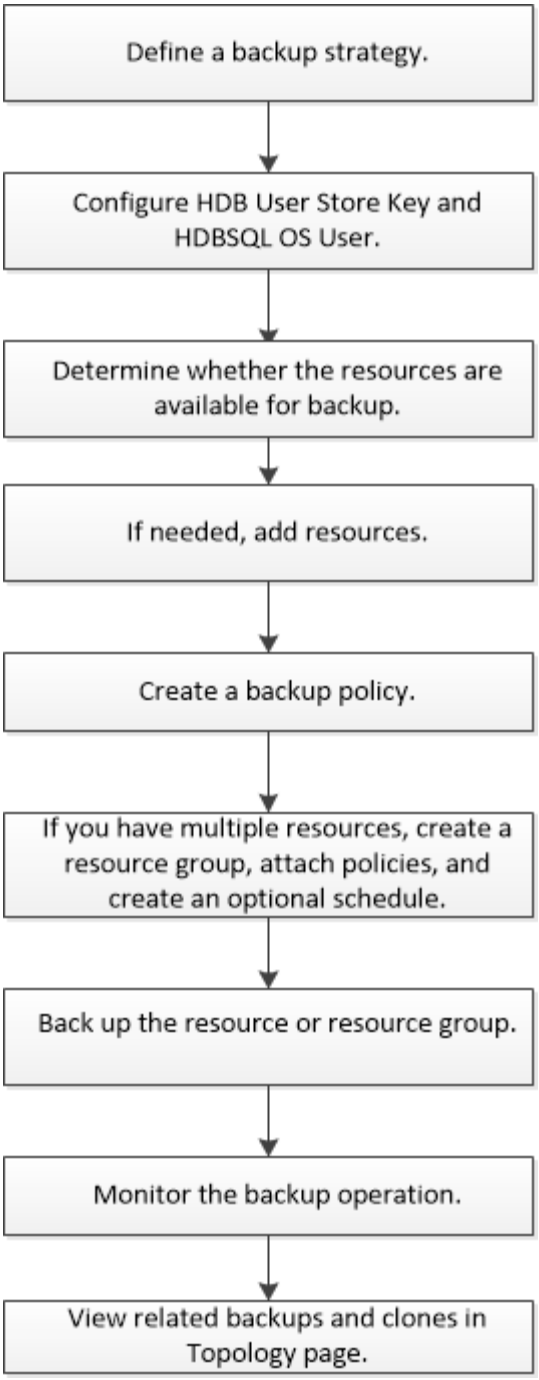
Pense em um grupo de recursos como definindo o que você quer proteger e quando você quer protegê-lo em termos de dia e tempo. Pense em uma política como definir como você deseja protegê-la. Se você estiver fazendo backup de todos os bancos de dados, por exemplo, poderá criar um grupo de recursos que inclua todos os bancos de dados no host. Em seguida, você pode anexar duas políticas ao grupo de recursos: Uma política diária e uma política por hora. 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 de bancos de dados para backup, gerenciamento de políticas de backup, criação de grupos de recursos e inclusão 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 clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell. "Guia de referência de cmdlet do software SnapCenter".

Configure a chave do armazenamento de usuários HDB e o usuário do sistema operacional HDBSQL para o banco de dados SAP HANA

Você deve configurar a chave do armazenamento de 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 HDB e o usuário SQL do HDB configurado, um ícone de cadeado vermelho será exibido apenas para os recursos autodescobertos. Se, durante uma operação de descoberta subsequente, a chave de armazenamento de usuário segura HDB configurada estiver incorreta ou não tiver fornecido acesso ao próprio banco de dados, o ícone de cadeado vermelho será reexibido.
- Você deve configurar a chave de armazenamento de usuário seguro HDB e o usuário 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 HDB SQL os User para acessar o banco de dados do sistema. Se o HDB SQL os User estiver configurado para acessar somente o banco de dados de locatário, a operação de descoberta falhará.

Passos

1. No painel de navegação à esquerda, clique em **Resources** 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.

   Em seguida, pode clicar para fechar o painel de filtro.
4. Selecione o banco de dados e clique em **Configurar banco de dados**.
5. Na seção Configurar configurações da base de dados, digite HDB Secure User Store Key.

   O nome do host do plug-in é exibido e o usuário do HDB SQL os é preenchido automaticamente para o <sid>.
6. Clique em **OK**.

Pode modificar a configuração da base de dados a partir da página topologia.

Descubra recursos e prepare contentores de banco de dados multitenant para proteção de dados

Descubra os bancos de dados automaticamente

Os recursos são bancos de dados SAP HANA e volume não-dados no host Linux gerenciado 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 do SAP HANA que estão disponíveis.

Antes de começar

- Você já deve ter concluído tarefas como instalar o servidor SnapCenter, adicionar a chave de armazenamento de usuários HDB, adicionar hosts e configurar as conexões do sistema de armazenamento.
- Você deve ter configurado o HDB Secure User Store Key e o usuário HDB SQL os no host Linux.
  - Tem de configurar a chave de armazenamento de utilizadores HDB com o utilizador SID adm. Por exemplo, para o sistema HANA com A22 como SID, a chave de armazenamento de usuário HDB deve ser configurada com a22adm.

- O plug-in do SnapCenter para banco de dados SAP HANA não oferece suporte à descoberta automática dos recursos residentes em ambientes virtuais RDM/VMDK. Você deve fornecer as informações de storage para ambientes virtuais e adicionar os bancos de dados manualmente.

Sobre esta tarefa

Depois de instalar o plug-in, todos os recursos nesse host Linux são automaticamente descobertos e exibidos na página recursos.

Os recursos descobertos automaticamente não podem ser modificados ou excluídos.

Passos

1. No painel de navegação à esquerda, clique em **Resources** 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 selecione o nome do host.

   Em seguida, pode clicar em * * para fechar o painel do filtro.
4. Clique em **Atualizar recursos** para descobrir os recursos disponíveis no host.

   Os recursos são exibidos juntamente 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, então não protegido será exibido na coluna Estado geral.
   - Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, e se não houver operação de backup executada, o Backup não executado será exibido na coluna Estado geral. O status mudará para Backup failed ou Backup successful com base no último status de backup.

Se o banco de dados SAP HANA não tiver uma chave de armazenamento de usuário segura HDB configurada, um ícone de cadeado vermelho será exibido ao lado do recurso. Se, durante uma operação de descoberta subsequente, a chave de armazenamento de usuário segura HDB configurada estiver incorreta ou não tiver fornecido acesso ao próprio banco de dados, o ícone de cadeado vermelho será reexibido.

Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

Depois de terminar

Você deve configurar a chave de armazenamento de usuário seguro HDB e o usuário HDBSQL os para poder proteger o banco de dados ou adicioná-lo ao grupo de recursos para executar operações de proteção de dados.

"Configure a chave do armazenamento de usuários HDB e o usuário do sistema operacional HDBSQL para o banco de dados SAP HANA"

Preparar contentores de banco de dados multitenant para proteção de dados

Para hosts SAP HANA diretamente registrados no SnapCenter, a instalação ou atualização do plug-in do SnapCenter para o banco de dados SAP HANA acionará uma descoberta automática de recursos no host. Depois de instalar ou atualizar o plug-in, para cada recurso de contentores de banco de dados multitenant (MDC) localizado no

host do plug-in, outro recurso MDC será automaticamente descoberto 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 final do período de retenção. Após o período de retenção expirar, você pode excluir o recurso MDC antigo 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 etapas a seguir 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 recurso MDC antigo com backups adicionados à versão anterior do SnapCenter e coloque-o em "modo de manutenção" na página topologia.

   Se o recurso for parte de um grupo de recursos, coloque o grupo de recursos em "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 servidor SnapCenter 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, horários 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 recurso MDC antigo da página recursos.

   Por exemplo, se o período de retenção de snapshots primários for de 7 dias e a retenção de snapshots secundários for de 45 dias, após 45 dias estarem concluídos e após todos os backups serem excluídos, você deverá excluir o grupo de recursos e o recurso MDC antigo.

Informações relacionadas

"Configure a chave do armazenamento de usuários HDB e o usuário do sistema operacional HDBSQL para o banco de dados SAP HANA"

"Veja os backups e clones do banco de dados SAP HANA na página topologia"

Adicione recursos manualmente ao host do plug-in

A deteção automática não é compatível com determinadas instâncias HANA. Você deve adicionar esses recursos manualmente.

Antes de começar

- Você deve ter concluído tarefas, como instalar o servidor SnapCenter, adicionar hosts, configurar conexões do sistema de armazenamento e adicionar a chave de armazenamento de usuários HDB.
- Para a replicação do sistema SAP HANA, recomenda-se adicionar todos os recursos desse sistema HANA a um grupo de recursos e fazer um backup em grupo de recursos. Isso garante um backup contínuo durante o modo de recuperação de falhas.

"Crie grupos de recursos e anexe políticas".

Sobre esta tarefa

A deteção 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 são suportadas por esses recursos.

- Configuração de vários host HANA
- Várias instâncias no mesmo host
- Replicação do SISTEMA HANA com escalabilidade horizontal de várias camadas
- Ambiente de replicação em cascata no modo de replicação do sistema

Passos

1. No painel de navegação à esquerda, selecione o plug-in do 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 recurso	Introduza o tipo de recurso. Os tipos de recursos são recipiente único, recipiente de banco de dados multitenant (MDC) e volume não-dados.
Nome do sistema HANA	Introduza o nome descritivo do sistema SAP HANA. Esta opção está disponível apenas se você selecionou tipos de recurso Single Container ou MDC.
SID	Introduza a 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	Digite a chave para se conetar ao sistema SAP HANA. A chave contém as informações de login para se conetar 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 HDBSQL os	Introduza o nome de utilizador para o qual a chave de armazenamento de utilizador seguro HDB está configurada. Para o Windows, é obrigatório que o usuário do sistema HDBSQL os seja o usuário DO SISTEMA. Portanto, você deve configurar a chave de armazenamento de usuário seguro HDB para o usuário DO SISTEMA.

4. Na página fornecer espaço físico 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 **Finish**.

   Os bancos de dados são exibidos juntamente com informações como SID, host de plug-in, grupos e políticas de recursos associados e status geral

Se você quiser fornecer aos usuários acesso a recursos, você deve atribuir os recursos aos usuários. Isso permite que os usuários executem as ações para as quais eles têm permissões nos ativos que são atribuídos a eles.

"Adicione um usuário ou grupo e atribua funções e ativos"

Depois de adicionar os bancos de dados, você pode modificar os detalhes do banco de dados do SAP HANA.

Não é possível modificar o seguinte se houver backups associados ao recurso SAP HANA:

- Contentores de banco de dados multitenant (MDC): SID, ou HDBSQL Client (plug-in) Host
- Contentor único: SID ou HDBSQL Client (plug-in) Host
- Volume não-dados: Nome do recurso, SID associado ou anfitrião Plug-in

Criar políticas de backup para bancos de dados SAP HANA

Antes de usar o SnapCenter para fazer backup dos recursos do banco de dados do SAP HANA, você precisa 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 retém backups.

Antes de começar

- Você precisa 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 precisa se preparar para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, configurar conexões do sistema de storage e adicionar recursos.
- O administrador do SnapCenter deve ter atribuído os SVMs para os volumes de origem e destino a você se estiver replicando snapshots em um espelho ou cofre.

  Além disso, você pode especificar as configurações de replicação, script e aplicativo na política. Essas opções economizam tempo quando você deseja reutilizar a política para outro grupo de recursos.

- Reveja os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror. Para obter informações, "Limites de objetos para sincronização ativa do SnapMirror"consulte .

Sobre esta tarefa

- Replicação do sistema SAP HANA
  - Você pode proteger o sistema principal do SAP HANA 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, toda a operação de proteção de dados pode ser executada à medida que o sistema SAP HANA secundário se torna o sistema SAP HANA primário.

  Você não pode criar um backup para o volume de dados do SAP HANA, mas o SnapCenter continua a proteger os volumes que não são de dados (NDV).

- SnapLock
  - Se a opção 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na política.
  - Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

As configurações do SnapLock primário são gerenciadas na política de backup do SnapCenter e as configurações do SnapLock secundário são gerenciadas pelo ONTAP.

Passos

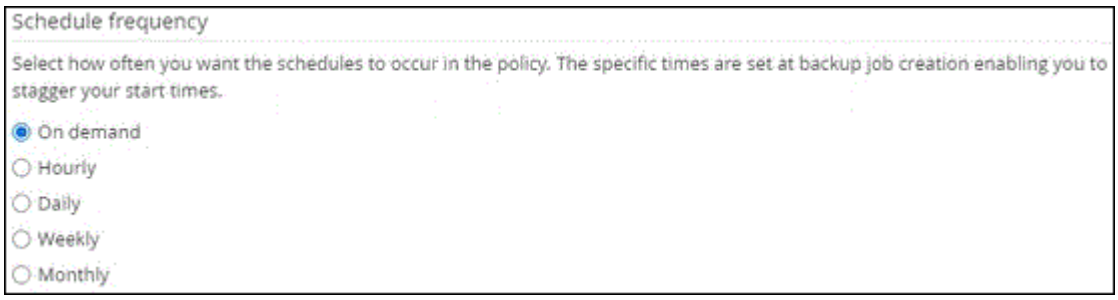
1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **políticas**.
3. Clique em **novo**.

4. Na página Nome, insira o nome e a descrição da política.
5. Na página Configurações, execute as seguintes etapas:
   - Escolha o tipo de cópia de segurança:

Se você quiser…	Faça isso…
Efetue uma verificação de integridade da base de dados	Selecione **Backup baseado em arquivos**. Somente os locatários ativos são copiados.
Crie um backup usando a tecnologia Snapshot	Selecione **Snapshot based**.

   - Especifique o tipo de agendamento selecionando **on demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.

> Você pode especificar a programação (data de início, data de término e frequência) para a operação de backup enquanto cria 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 programações de backup a cada política.



> Se você tiver agendado para as 2:00 da manhã, o horário não será acionado durante o horário de verão (DST).

   - Na seção **Configurações personalizadas de backup**, forneça quaisquer configurações específicas de backup que tenham que ser passadas para o formato de valor de chave do plug-in.

     Você pode fornecer vários valores-chave a serem passados para o plug-in.

6. Na página retenção, 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 instantâneos	Selecione **Total de cópias Snapshot a manter** e especifique o número de capturas instantâneas que deseja manter. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro. O valor máximo de retenção é 1018 para recursos no ONTAP 9.4 ou posterior e 254 para recursos no ONTAP 9.3 ou anterior. Os backups falharão se a retenção for definida para um valor maior do que o que a versão subjacente do ONTAP suporta. Para backups baseados em cópias Snapshot, defina a contagem de retenção para 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino. Para replicação do sistema SAP HANA, recomenda-se adicionar todos os recursos do sistema SAP HANA a um grupo de recursos. Isso garante que o número certo de backups seja retido. 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 está definida como 7 para um grupo de recursos com SAP HANA System Replication primário e SAP HANA System Replication secundário. Você pode tirar um máximo de 7 snapshots de cada vez, incluindo SAP HANA System Replication Primary e SAP HANA System Replication secundário.

Se você quiser…	Então…
Mantenha as capturas instantâneas por um determinado número de dias	Selecione **manter cópias Snapshot para** e especifique o número de dias para os quais deseja manter as capturas instantâneas antes de excluí-las.
Período de bloqueio de cópias snapshot	Selecione período de bloqueio de cópias instantâneas e selecione dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

7. Para backups baseados em cópia Snapshot, especifique as configurações de replicação na página replicação:

Para este campo…	Faça isso…
Atualizar SnapMirror depois de criar uma cópia Snapshot local	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Esta opção deve estar ativada para a sincronização ativa do SnapMirror. Se a relação de proteção no ONTAP for do tipo espelho e Cofre e se você selecionar somente essa opção, a captura Instantânea criada no primário não será transferida para o destino, mas será listada no destino. Se esta captura Instantânea for selecionada no destino para executar uma operação de restauração, a localização secundária não estará disponível para a mensagem de erro de backup abobadado/espelhado selecionada 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. "Veja os backups e clones do banco de dados SAP HANA na página topologia"Consulte .

Para este campo…	Faça isso…
Atualizar SnapVault depois de criar uma cópia Snapshot local	Selecione esta opção para executar a replicação de backup disco a disco (backups 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 apenas no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página topologia atualiza o período de bloqueio no secundário que é recuperado do ONTAP. Para obter mais informações sobre o SnapLock Vault, consulte "Armazene cópias Snapshot em WORM em um destino de cofre" "Veja os backups e clones do banco de dados SAP HANA na página topologia"Consulte .
Etiqueta de política secundária	Selecione uma etiqueta Snapshot. Dependendo do rótulo de captura instantânea selecionado, o ONTAP aplica a política de retenção de snapshot secundária que corresponde ao rótulo. Se você selecionou **Atualizar SnapMirror depois de criar uma cópia Snapshot local**, você pode especificar opcionalmente o rótulo de política secundária. No entanto, se você selecionou **Atualizar SnapVault depois de criar uma cópia Snapshot local**, especifique o rótulo de política secundária.
Contagem de tentativas de erro	Introduza o número máximo de tentativas de replicação que podem ser permitidas antes de a operação parar.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o storage secundário para evitar atingir o limite máximo de snapshots no storage secundário.

8. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas

Um grupo de recursos é o contentor ao qual você deve adicionar recursos que deseja fazer backup e proteger. Um grupo de recursos permite fazer 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 tarefa de proteção de dados que deseja executar.

Sobre esta tarefa

- Para criar backups de replicação do sistema SAP HANA, recomenda-se adicionar todos os recursos do sistema SAP HANA a um grupo de recursos. Isso garante um backup contínuo durante o modo de recuperação de falhas.
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.
- A adição de novos bancos de dados sem a sincronização ativa do SnapMirror a um grupo de recursos existente que contenha recursos com a sincronização ativa do SnapMirror não é suportada.
- A adição de novos bancos de dados a um grupo de recursos existente no modo failover da sincronização ativa do SnapMirror não é suportada. Você pode adicionar recursos ao grupo de recursos apenas no estado regular ou de failback.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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	Introduza um nome para o grupo de recursos. O nome do grupo de recursos não deve exceder 250 carateres.
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.

Para este campo…	Faça isso…
Use o formato de nome personalizado para cópia Snapshot	Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea. Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um carimbo de data/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 **Resource Type**.

   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:

      Ative o backup do grupo de consistência e execute as seguintes tarefas:

Para este campo…	Faça isso…
Tenha tempo para esperar que a operação de snapshot do grupo de consistência seja concluída	Selecione **urgente**, **Médio** ou **relaxado** para especificar o tempo de espera para que a operação Snapshot seja concluída. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a 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 quiesce, Snapshot e unquiesce. Também pode introduzir os pré comandos a serem executados antes de sair em caso de falha.

b. Clique na seta **Custom Configurations** (Configurações personalizadas) e insira os pares de valor de chave personalizados necessários para todas as operações de proteção de dados usando esse recurso.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_ENABLE	(Y/N)	Permite que a gestão do registo de arquivo elimine os registos de arquivo.
ARCHIVE_LOG_RETENÇÃO	number_of_days	Especifica o número de dias em que os logs de arquivo são mantidos. Esta definição tem de ser igual ou superior a NTAP_SNAPSHOT_ RETENÇÕES.
ARCHIVE_LOG_DIR	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs do arquivo.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_EXT	extensão_ficheiro	Especifica o comprimento da extensão do arquivo de log do arquivo. Por exemplo, se o log de arquivo 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.
ARCH ARCHIVE_LOG_RECURSIVE_ SE	(Y/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs do arquivo estiverem localizados em subdiretórios.

Os pares de valor de chave personalizados são compatíveis com sistemas plug-in SAP HANA Linux e não são compatíveis com banco de dados SAP HANA registrado como um plug-in centralizado do Windows.

c. Clique na seta **Snapshot Copy Tool** 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 instantâneo. Para recursos do Linux, essa opção não é aplicável.	Selecione **SnapCenter com consistência do sistema de arquivos**. Esta opção não é aplicável ao plug-in SnapCenter para banco de dados SAP HANA.
SnapCenter para criar um instantâneo no nível de storage	Selecione **SnapCenter sem consistência do sistema de arquivos**.
Para inserir o comando a ser executado no host para criar cópias Snapshot.	Selecione **Other** e digite o comando a ser executado no host para criar uma captura Instantânea.

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 programações para políticas selecionadas.

b. Na coluna Configurar agendas, clique em + para a política que deseja configurar.

c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e clique em **OK**.

Onde, policy_name é o nome da política selecionada.

As programações configuradas são listadas na coluna **programações aplicadas**.

As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas 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 **Finish**.

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para banco de dados SAP HANA

Você deve criar uma conexão de máquina virtual de storage (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 Administrador da infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estão em andamento.

  As instalações de plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento, pois 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 do sistema de armazenamento devem ser exclusivos.

  O SnapCenter não é compatível com vários sistemas de storage com o mesmo nome em clusters diferentes. Cada sistema de storage com suporte do SnapCenter deve ter um nome exclusivo e um endereço IP de 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 servidor SnapCenter.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode hana
```

5. Instale o pacote e o plug-in do SnapCenter para o 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Fazer backup de bancos de dados do SAP HANA

Se um recurso ainda não fizer parte de qualquer 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 uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.
- Para a operação de backup baseada em cópia Snapshot, certifique-se de que todos os bancos de dados do locatário estejam válidos e ativos.
- Para criar backups de replicação do sistema SAP HANA, recomenda-se adicionar todos os recursos do sistema SAP HANA a um grupo de recursos. Isso garante um backup contínuo durante o modo de recuperação de falhas.

  "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 locatário estiverem inativos, defina o parâmetro ALLOW_FILE_BASED_BACKUP_IFINACTIVO_TENANTS_PRESENT como **YES** no arquivo de propriedades 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*. Em alternativa, pode também consultar "Guia de referência de cmdlet do software SnapCenter"

- Para comandos pré e POST para operações quiesce, Snapshot e unquiesce, você deve verificar se os comandos existem na lista de comandos disponível no host plug-in dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização padrão no host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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, em seguida, selecione o nome do host e o tipo de recurso para filtrar os recursos. Em seguida, pode selecionar para fechar o painel de filtro.
3. Selecione o recurso que você deseja fazer backup.
4. Na página recurso, selecione **Use o formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.
5. Na página Configurações do aplicativo, faça o seguinte:
   - Selecione a seta **backups** para definir opções adicionais de backup:

     Ative o backup do grupo de consistência, se necessário, e execute as seguintes tarefas:

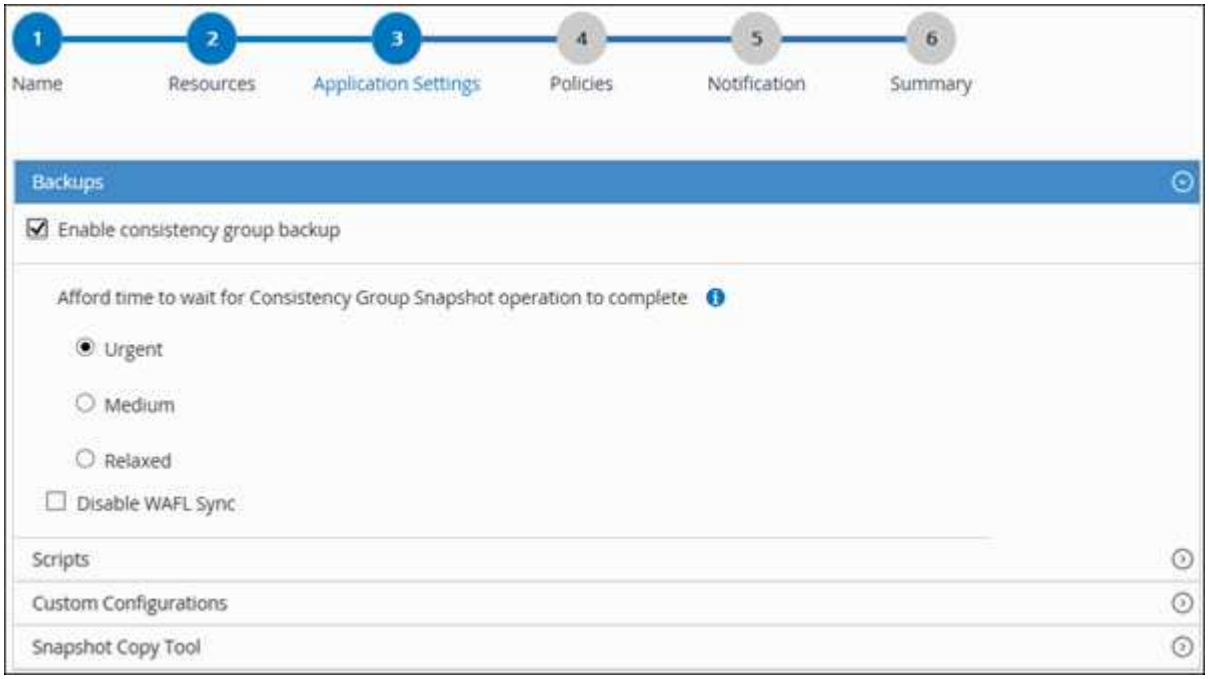
Para este campo…	Faça isso…
Tenha tempo para esperar a conclusão da operação "Consistency Group Snapshot"	Selecione **urgente**, **Médio** ou **relaxado** para especificar o tempo de espera para que a operação Snapshot termine. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL.

   - Selecione a seta **Scripts** para executar comandos pré e POST para operações quiesce, Snapshot e unquiesce.

     Você também pode executar pré-comandos antes de sair da operação de backup. Os Prescripts e postscripts são executados no servidor SnapCenter.
   - Selecione a seta **Custom Configurations (Configurações personalizadas) e, em seguida, insira os pares de valores personalizados necessários para todos os trabalhos que usam esse recurso.
   - Selecione a seta **Snapshot Copy Tool** para selecionar a ferramenta para criar instantâneos:

Se você quiser…	Então…
SnapCenter para criar um Snapshot no nível de storage	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 instantâneo	Selecione **SnapCenter com consistência do sistema de arquivos**.
Para inserir o comando para criar uma captura Instantânea	Selecione **Other** e, em seguida, digite o comando para criar uma captura Instantânea.



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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Selecione + * * na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e selecione **OK**.

      policy_name é o nome da política selecionada.

   As programações configuradas são listadas na coluna agendas aplicadas.

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 **Finish**.

   A página de topologia de recursos é exibida.

9. Selecione **fazer uma cópia de segurança 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. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.
    - Nas configurações do MetroCluster, o SnapCenter pode não ser capaz de detetar uma relação de proteção após um failover.

      Para obter informações, consulte: "Não é possível detetar a relação SnapMirror ou SnapVault após o failover do MetroCluster"

    - Se você estiver fazendo backup de dados de aplicativos em VMDKs e o tamanho de heap Java para o plug-in SnapCenter para VMware vSphere não for grande o suficiente, o backup pode 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 servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

   ```
   Open-smconnection  -SMSbaseurl
   https:\\snapctr.demo.netapp.com:8146\
   ```

   É apresentado o aviso de nome de utilizador e palavra-passe.

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 que não seja de 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 Snapshot:

   ```
   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 arquivos:

   ```
   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 contentor:

```
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 não-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 da tarefa (em execução, concluída ou com falha) usando o cmdlet Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Monitore os detalhes da tarefa de backup, como ID do backup, nome do backup para executar a operação de restauração ou clone 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*. Em alternativa, pode também consultar o "Guia de referência de 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 uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, 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 uma programação configurada, os backups ocorrerão automaticamente de acordo com a programação.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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 selecionando a tag. Em seguida, pode 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. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Monitore operações de backup de bancos de dados SAP HANA

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado correspondente das operações:

-

Em curso

- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- 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 a que apenas as operações de cópia de segurança sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Backup**.
   d. Na lista suspensa **Status**, selecione o status da cópia de segurança.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.

   Embora o status do trabalho de backup seja exibido , quando você clica nos detalhes do trabalho, você pode ver que algumas das tarefas secundárias da operação de backup ainda estão em andamento ou marcadas com sinais de aviso.

5. Na página Detalhes da tarefa, clique em **Exibir logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Monitore operações de proteção de dados em bancos de dados SAP HANA no painel atividade

O painel atividade exibe as cinco operações mais recentes executadas. O painel atividade também é exibido quando a operação foi iniciada e o status da operação.

O painel atividade exibe informações sobre operações de backup, restauração, clone e backup agendadas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 da tarefa**.

Cancelar operações de backup para SAP HANA

Você pode cancelar as operações de backup que estão na fila.

O que você vai precisar

- Você deve estar logado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de cópia de segurança em execução.
- Você pode usar os comandos GUI, cmdlets do SnapCenter ou CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** está desativado 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 em fila de outros membros enquanto usa essa função.

Passos

1. Execute uma das seguintes ações:

A partir 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 da atividade	a. Depois de iniciar a operação de backup, clique em no painel atividade para exibir as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

A operação é cancelada e o recurso é revertido para o estado anterior.

Veja os backups e clones do banco de dados SAP HANA na página topologia

Ao se preparar para fazer backup ou clonar um recurso, talvez seja útil exibir uma representação gráfica de todos os backups e clones no storage primário e secundário.

Sobre esta tarefa

Você pode revisar os ícones a seguir na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no storage primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups e clones disponíveis no storage primário.
- Exibe o número de backups e clones espelhados no storage secundário usando a tecnologia SnapMirror.

- Exibe o número de backups e clones replicados no storage secundário usando a tecnologia SnapVault.

  O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou backups 6 usando uma política para reter apenas 4 backups, o número de backups exibidos é 6.

Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

Na página topologia, você pode ver todos os backups e clones disponíveis para o grupo de recursos ou recursos selecionado. Você pode visualizar os detalhes desses backups e clones e, em seguida, selecioná-los para executar operações de proteção de dados.

Se você tiver uma relação secundária como sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), você poderá ver os seguintes ícones adicionais:

- O site da réplica está em cima.
- O site da réplica está inativo.
- A relação do espelho secundário ou do cofre não foi restabelecida.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o recurso ou o 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 de 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 arquivos, backups baseados em cópia Snapshot e clones.

   Clicar no botão **Refresh** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clique no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Um horário semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo é espalhado por vários volumes, o tempo de expiração do SnapLock para o backup será o tempo de expiração do SnapLock mais longo definido para um snapshot em um volume. O tempo de expiração mais longo do SnapLock é recuperado do ONTAP.

   Para a 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 a relação de sincronização ativa do SnapMirror.

- Para a sincronização ativa do SnapMirror e somente para o ONTAP 9.14,1, as relações de espelhamento do Async ou EspelrorVault do Async com o novo destino primário devem ser configuradas manualmente após o failover. A partir do ONTAP 9.15,1 em diante, o espelho do Async ou o MirrorVault do Async 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 **Refresh** somente depois que um backup tiver sido criado.

5. No modo de 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 um 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 estão no armazenamento secundário.

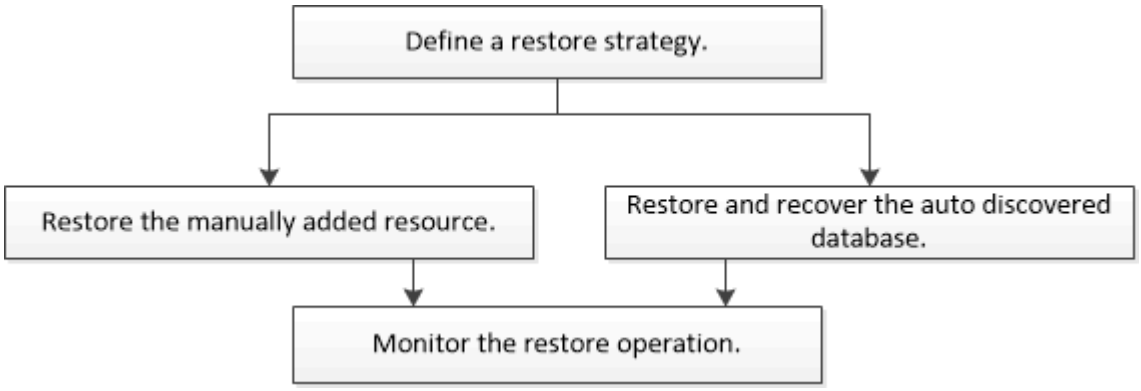
7. Se quiser excluir um clone, selecione-o na tabela e clique em .
8. Se quiser dividir um clone, selecione-o na tabela e clique em .

Restaure os bancos de dados do SAP HANA

Restaure o fluxo de trabalho

O fluxo de trabalho de restauração e recuperação inclui Planejamento, execução das 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 clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre cmdlets do PowerShell.

"Guia de referência de cmdlet do software SnapCenter".

Restaure e recupere um backup de recursos 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 dos grupos de recursos ou recursos.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos pré-restauração, pós restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização 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

- As cópias de backup baseadas em arquivo não podem ser restauradas a partir 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 precisa usar scripts de recuperação HANA ou estúdio externos ao SnapCenter para recuperar os backups feitos no SnapCenter 4,2.
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage 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 no local principal.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com o tipo, host, grupos de recursos e políticas associados e status.

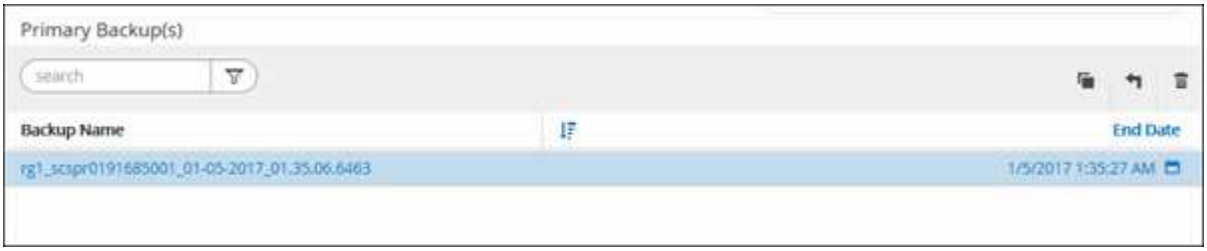
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, ""não protegido"" é exibido na coluna Estado geral. Isso pode significar que o recurso não está protegido ou que o recurso foi protegido 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 do recurso é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Na tabela de backup principal, selecione o backup do qual você deseja restaurar e clique em * * .



6. Na página Restaurar escopo, selecione **recurso completo** ou **nível de arquivo**.

   a. Se você selecionar **Complete Resource**, todos os volumes de dados configurados do banco de dados SAP HANA serão restaurados.

      Se o recurso contiver volumes ou qtrees, os instantâneos obtidos 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.

   b. Se você selecionar **File Level**, poderá selecionar **All** 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.

        Pode selecionar vários LUNs.

Se você selecionar **All**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.

7. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar 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 a execução de 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 **Finish**.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 29th 2015 de janeiro a 3rd 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 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Restaure e recupere 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 dos grupos de recursos ou recursos.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos pré-restauração, pós restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter*

Plug-in Creator/etc/allowed_commands.config

- Localização 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

- As cópias de backup baseadas em arquivo não podem ser restauradas a partir 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 precisa usar scripts de recuperação HANA ou estúdio 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 instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage 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 no local principal.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com o tipo, host, grupos de recursos e políticas associados e status.

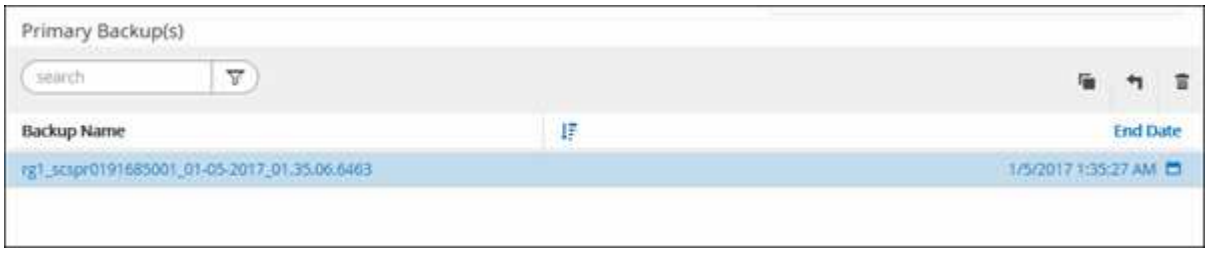
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, ""não protegido"" é exibido na coluna Estado geral. Isso pode significar que o recurso não está protegido ou que o recurso foi protegido 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 do recurso é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Na tabela de backup principal, selecione o backup do qual você 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 **Complete Resource** (com ou sem **volume Revert**) ou **Tenant Database**.

A operação de recuperação não é suportada pelo servidor SnapCenter para vários locatários quando o usuário seleciona a opção **Banco de dados do locatário** 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 todo o volume.

   Essa opção está disponível para backups feitos no SnapCenter 4,3 em ambientes NFS.

   Se o recurso contiver volumes ou qtrees, os instantâneos obtidos 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. Isso é aplicável quando a opção **Complete Resource** com **volume Revert** estiver selecionada para restauração.

b. Selecione **Banco de dados do locatário**.

   Esta opção está disponível apenas para recursos 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 do locatário**, use O estúdio HANA ou use scripts de recuperação HANA externos ao SnapCenter para executar a operação de recuperação.

7. Na página âmbito de recuperação, selecione uma das seguintes opções:

Se você…	Faça isso…
Deseja recuperar o mais próximo possível da hora atual	Selecione **Recover to most recent State** (recuperar para o estado mais recente). Para recursos de contentor único, especifique um ou mais locais de backup de log e catálogo. Para recursos de contentor de banco de dados multitenant (MDC), especifique um ou mais locais de backup de log e o local do catálogo de backup. Para recursos MDC, o caminho deve conter Registros de banco de dados de sistema e banco de dados de locatário.

Se você…	Faça isso…
Deseja recuperar para o ponto especificado no tempo	Selecione **Recover to point in time**. a. Selecione o fuso horário. O fuso horário do navegador é preenchido por padrão. O fuso horário selecionado juntamente com a hora de entrada é convertido para GMT absoluto. b. Introduza 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 ambos os locais é de 3 horas, e como o usuário fez login em Raleigh, NC, o fuso horário padrão do navegador que será selecionado na GUI é GMT-04:00. Se o usuário quiser executar uma recuperação para 5 a.m .Sunnyvale, CA, então o usuário deve definir o fuso horário do navegador para o fuso horário do host DO HANA Linux, que é GMT-07:00 e especificar a data e a hora como 5:00 a.m. Para recursos de contentor 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 MDC, o caminho deve conter Registros de banco de dados de sistema e banco de dados de locatário.
Deseja recuperar para um backup de dados específico	Selecione **Recover to specified data backup**.
Não quero recuperar	Selecione **sem recuperação**. Você deve executar a operação de recuperação manualmente a partir do estúdio HANA.

Você pode recuperar apenas os backups que são 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 a conversão ou descoberta do recurso como recurso descoberta automática.

8. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar 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 a execução de 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 **Finish**.
12. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Restaure recursos usando cmdlets do PowerShell

A restauração de um backup de recurso inclui iniciar uma sessão de conexão com o servidor SnapCenter, listar os backups e recuperar informações de backup e 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 servidor SnapCenter 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 29th 2015 de janeiro a 3rd 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 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Monitore as operações de restauração de bancos de dados SAP HANA

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um 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 executar.

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso

- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Restore**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Clonar backups de recursos do SAP HANA

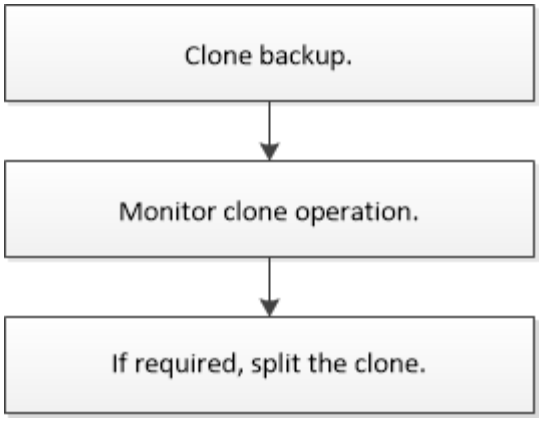
Fluxo de trabalho clone

O fluxo de trabalho do clone inclui a execução da operação de clone e o monitoramento da 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 de aplicativos
  - 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 clone:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre cmdlets do PowerShell.

Clone um backup de banco de dados SAP HANA

Você pode usar o SnapCenter para clonar um backup. Você pode clonar 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 storage (SVM).
- Não é possível clonar backups baseados em arquivo.
- O servidor clone de destino deve ter o mesmo SID de instância do SAP HANA que é fornecido no campo SID Clone de destino.
- Para comandos pré-clone ou pós-clone, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos 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 limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .
- Para o ONTAP 9.12,1 e versão anterior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com informações como tipo, host, grupos e políticas de recursos associados e status.

3. Selecione o grupo de recursos ou recursos.

   Você deve selecionar um recurso se selecionar um grupo de recursos.

   A página de topologia do grupo de recursos ou recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Selecione o backup de dados na tabela e clique em .
6. Na página localização, execute as seguintes ações:

Para este campo…	Faça isso…
Host plug-in	Selecione o host no qual o clone deve ser montado e o plug-in está instalado.
SID Clone alvo	Insira o ID da instância do SAP HANA para clonar dos backups existentes.
Endereço IP de exportação NFS	Insira endereços IP ou os nomes de host nos quais os volumes clonados serão exportados.
Iniciador iSCSI	Insira o nome do iniciador iSCSI do host para o qual os LUNs são exportados. Esta opção só está disponível se você selecionou o tipo de recurso LUN.
Protocolo	Introduza o protocolo LUN. Esta opção só está disponível se você selecionou 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 fonte pode ter vários volumes de destino.

   Antes da clonagem, você deve garantir que o iniciador iSCSI ou o FCP estejam presentes e configurados e conetados em hosts alternativos.

7. Na página Scripts, execute as seguintes etapas:

   Os scripts são executados no host do plug-in.

a. Digite os comandos para pré-clone ou pós-clone que devem ser executados antes ou depois da operação clone, respetivamente.
   - Comando pre clone: Exclua bancos de dados existentes com o mesmo nome
   - Comando Post clone: Verifique um banco de dados ou inicie um banco de dados.

b. Digite o comando mount para montar um sistema de arquivos em um host.

   Monte o comando 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 **Finish**.
10. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 clone 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 clone a partir de um backup existente e especifique os endereços IP de exportação NFS nos quais os volumes clonados são 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 clone.

4. Verifique se os backups foram clonados com sucesso usando o cmdlet Get-SmCloneReport para exibir os detalhes da tarefa clone.

   Você pode exibir 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 clone de banco de dados SAP HANA

Você pode monitorar o andamento das operações de clone do SnapCenter usando a página tarefas. Você pode querer verificar o progresso de uma operação para determinar

quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista para que apenas operações de clone sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Divida um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido torna-se independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clones em um clone intermediário.

  Por exemplo, depois de criar clone1 a partir de um backup de banco de dados, você pode criar um backup de clone1 e clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e não é possível executar a operação de divisão de clones no clone1. No entanto, você pode executar a operação de divisão de clones no clone2.

  Depois de dividir clone2, você pode executar a operação de divisão de clones no clone1 porque clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e as tarefas de clone do clone são excluídas.
- Para obter informações sobre limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .

- Certifique-se de que o volume ou o agregado no sistema de storage esteja on-line.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página **recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicativos 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 do recurso é exibida.

4. No modo de 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 deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

   A operação de divisão de clones deixa de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clones e tentar novamente a operação de divisão de clones.

   Se você quiser um tempo de enquete mais longo 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 que o SMCore busque o status da operação de divisão de clones. O valor é em milissegundos e o valor padrão é de 5 minutos.

   Por exemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

   A operação de inicialização dividida de clone falhará se o backup, a restauração ou outra divisão de clones estiver em andamento. Você deve reiniciar a operação de divisão de clones somente depois que as operações em execução estiverem concluídas.

Informações relacionadas

"O clone ou a verificação do SnapCenter falha com o agregado não existe"

Exclua ou divida clones do banco de dados do SAP HANA após a atualização do SnapCenter

Após a atualização para o SnapCenter 4,3, você não verá mais os clones. Você pode excluir o clone ou dividir os clones da página topologia do recurso a partir do qual os clones foram criados.

Sobre esta tarefa

Se você quiser localizar o espaço físico 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-sprotectresource.
4. Selecione o recurso pai na página recursos.

   A página de topologia do recurso é exibida.

5. Na visualização Gerenciar cópias, selecione os clones nos sistemas de storage primário ou secundário (espelhado ou replicado).
6. Selecione os clones e clique para excluir clones ou clique para dividir os clones.
7. Clique em **OK**.

Proteger 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 plug-in SnapCenter para banco de dados Oracle é um componente do lado do host do software NetApp SnapCenter que permite o gerenciamento de proteção de dados com reconhecimento de aplicações de bancos de dados Oracle.

O plug-in para banco de dados Oracle automatiza o backup, catalogação e desinstalação com o Oracle Recovery Manager (RMAN), verificação, montagem, desmontagem, restauração, recuperação e clonagem de bancos de dados Oracle em seu ambiente SnapCenter. O plug-in para banco de dados Oracle instala o plug-in do SnapCenter 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 que executam aplicativos SAP. No entanto, a integração SAP BR*Tools não é suportada.

- Faça backup de arquivos de dados, arquivos de controle e arquivos de log de arquivamento.

  A cópia de segurança é suportada apenas no nível da base de dados de contentores (CDB).

- Restauração e recuperação de bancos de dados, CDBs e bancos de dados conetáveis (PDBs).

  A recuperação incompleta de PDBs não é suportada.

- Crie clones de bancos de dados de produção até um ponto no tempo.

  A clonagem é suportada apenas no nível CDB.

- Verifique os backups imediatamente.
- Monte e desmonte os backups de dados e log para operação de recuperação.
- Agendar operações de backup e verificação.
- Monitorar todas as operações.
- Exibir relatórios para operações de backup, restauração e clone.

Recursos do Plug-in para banco de dados Oracle

O plug-in para banco de dados Oracle se integra ao banco de dados Oracle no host Linux ou AIX e com tecnologias NetApp no sistema de armazenamento.

- Interface gráfica do usuário unificada

  A interface do SnapCenter fornece padronização e consistência em plug-ins e ambientes. A interface do SnapCenter permite concluir operações consistentes de backup, restauração, recuperação e clone em plug-ins, usar relatórios centralizados, usar visualizações de dashboard rápidas, configurar controle de acesso baseado em funções (RBAC) e monitorar tarefas em todos os plug-ins.

- Administração central automatizada

  Você pode agendar operações de backup e clone, configurar a retenção de backup baseada em política e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- Tecnologia NetApp Snapshot sem interrupções

  O SnapCenter usa a tecnologia NetApp Snapshot com o plug-in para banco de dados Oracle e plug-in para UNIX para fazer backup de bancos de dados. Os snapshots consomem espaço mínimo de storage.

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)
- Delegação de funções centralizada e segurança compatível com RBAC

  Você também pode definir as credenciais para que os usuários autorizados do SnapCenter tenham permissões no nível do aplicativo.

- Suporte para gerenciamento de logs de arquivamento (ALM) para operações de restauração e clonagem
- Criação de cópias pontuais e com uso eficiente de espaço de bancos de dados de produção para teste ou extração de dados usando a tecnologia NetApp FlexClone

  É necessária uma licença FlexClone no sistema de storage onde você deseja criar o clone.

- Suporte ao recurso de grupo de consistência (CG) do ONTAP como parte da criação de backups em ambientes SAN e ASM
- Verificação de backup sem interrupções e automatizada
- Funcionalidade de executar vários backups simultaneamente em vários hosts de banco de dados

  Em uma única operação, os snapshots são consolidados quando os 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 em NFS e VMFS, e ASM em NFS, SAN, RDM e VMDK
- Suporte para o recurso de mapa LUN seletivo (SLM) do ONTAP

  Habilitado por padrão, o recurso SLM deteta 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 desativar isso definindo o valor do parâmetro ENABLE_LUNPATH_MONITORING como false.
  - Você pode especificar a frequência em que os caminhos LUN serão corrigidos automaticamente atribuindo o valor (em horas) ao parâmetro LUNPATH_MONITORING_INTERVAL. Para obter informações sobre o SLM, consulte "Guia de administração de SAN ONTAP 9".

- Suporte para memória não volátil Express (NVMe) no Linux
  - O NVMe útil deve ser instalado no host.

    É necessário instalar o NVMe util para clonar ou montar em um host alternativo.
  - Operações de backup, restauração, clone, montagem, desmontagem, catálogo, descatálogo e verificação são compatíveis com o hardware NVMe, exceto para ambientes virtualizados como RDM.

    As operações acima são suportadas em dispositivos sem partições ou com partição única.

    > Você pode configurar a solução multipathing para dispositivos NVMe definindo a opção multipathing nativa no kernel. O multipathing do Mapeador de dispositivos (DM) não é suportado.
  - Workflows de backup, restauração, clone, montar, desmontar, catalogar, descatalogar e verificar workflows são compatíveis com NVMe em TCP/IP.
  - Workflows de backup, restauração, clone, montar, desmontar, catalogar, descatalogar e verificar são compatíveis com o layout VMDK criado no NVMe sobre TCP/IP.
- É compatível com a sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), que permite que os serviços empresariais continuem operando mesmo em caso de falha completa do local, oferecendo suporte para failover transparente de aplicações usando uma cópia secundária. Nem a intervenção manual nem o script adicional são necessários 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 definir os usuários não padrão 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: oracle
  - DB_GROUP
  - GI_USER_grid
  - GI_GROUP: Instalação

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 storage antes de instalar o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX.

O SnapCenter não oferece suporte ao provisionamento de storage para Linux e AIX.

Tipos de armazenamento compatíveis com Linux

A tabela a seguir lista os tipos de armazenamento suportados no Linux.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados a FC • LUNs ligados ao iSCSI • Volumes conectados a NFS • NVMe-FC • NVMe/TCP
VMware ESXi	• LUNs RDM conetados por um FC ou iSCSI ESXi HAScanning de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluído 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** para 1 para reexaminar somente os HBA listados em HBA_DRIVER_NAMES. • ISCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI • VMDKs em armazenamentos de dados NFS • VMDKs no VMFS criado em NVMe/TCP O RAC é compatível com o ESX 8.0U2, que tem suporte para VMDK compartilhado • Volumes NFS conectados diretamente ao sistema convidado • Armazenamentos de dados da VVol em NFS e SAN O armazenamento de dados da VVol só pode ser provisionado com as Ferramentas do ONTAP para o VMware vSphere.

Tipos de storage compatíveis com AIX

A tabela a seguir lista os tipos de armazenamento suportados no AIX.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados a FC e iSCSI. Em um ambiente SAN, os sistemas de arquivos ASM, LVM e SAN são compatíveis. NFS no AIX e no sistema de arquivos não é suportado. • Sistema de arquivos Journaled aprimorado (JFS2) Suporta log in-line em sistemas de arquivos SAN e layout LVM.

O "Ferramenta de Matriz de interoperabilidade do NetApp" contém as informações mais recentes sobre as versões suportadas.

Preparar sistemas de storage para replicação SnapMirror e SnapVault para plug-in para Oracle

Você pode usar um plug-in do 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 disco a disco para conformidade com os padrões e outros fins relacionados à governança. Antes de executar essas tarefas, você deve configurar uma relação de proteção de dados entre os volumes de origem e destino e inicializar a relação.

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 . Se você estiver usando a sincronização ativa do SnapMirror , use os agendamentos padrão do SnapMirror ou SnapVault para a sincronização ativa do SnapMirror e para relacionamentos assíncronos.

Se você estiver vindo para o SnapCenter de um produto NetApp SnapManager e estiver satisfeito com as relações de proteção de dados que configurou, ignore esta seção.

Uma relação de proteção de dados replica dados no storage primário (o volume de origem) para o storage secundário (o volume de destino). Ao inicializar a relação, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não suporta relações em cascata entre volumes SnapMirror e SnapVault (**Primary** > **Mirror** > **Vault**). Você deve usar relacionamentos de fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis de versão e como configurá-los, consulte "Documentação do ONTAP".

Mínimo de ONTAP Privileges necessário para plug-in para Oracle

Os ONTAP Privileges mínimos necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

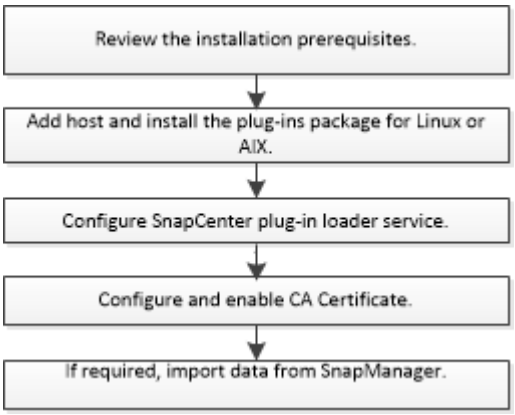
- Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
  - event generate-AutoSupport-log
  - mostra o histórico de trabalhos
  - paragem do trabalho
  - lun
  - show de atributo lun
  - lun criar
  - eliminação lun
  - geometria lun
  - lun igrop add
  - lun igrop criar
  - eliminação do agrupamento lun
  - mudar o nome do grupo lun
  - show de grupos de lun
  - nós complementares de mapeamento de lun
  - mapeamento lun criar
  - eliminação do mapeamento lun
  - mapeamento lun remove-reporting-nonos
  - mostra de mapeamento lun
  - modificação de lun
  - movimentação de lun no volume
  - lun offline
  - lun online
  - limpeza da reserva persistente de lun
  - redimensionar lun
  - série lun
  - mostra lun
  - regra adicional de política do SnapMirror
  - regra de modificação de política do SnapMirror
  - regra de remoção da política do SnapMirror
  - SnapMirror policy show
  - restauração de SnapMirror
  - SnapMirror show

- SnapMirror show-history
- atualização do SnapMirror
- SnapMirror update-ls-set
- SnapMirror lista-destinos
- versão
- clone de volume criar
- show de clone de volume
- início da divisão do clone de volume
- paragem dividida clone volume
- criar volume
- destruição de volume
- clone de arquivo de volume criar
- show-disk-use do arquivo de volume
- volume off-line
- volume online
- modificação do volume
- criar qtree de volume
- eliminação de qtree de volume
- modificação de qtree de volume
- apresentação de qtree de volume
- restrição de volume
- apresentação do volume
- criar instantâneo de volume
- eliminar instantâneo do volume
- modificação do instantâneo do volume
- mudar o nome do instantâneo do volume
- restauração de snapshot de volume
- restauração de arquivo de snapshot de volume
- apresentação de instantâneo do volume
- desmontar o volume
- svm
- svm cifs
- apresentação do shadowcopy cifs de svm
- mostra o svm
- interface de rede
- mostra da interface de rede
- MetroCluster show

Instale o plug-in do SnapCenter para o banco de dados Oracle

Fluxo de trabalho de instalação do plug-in SnapCenter para banco de dados Oracle

Você deve instalar e configurar o plug-in do SnapCenter para o banco de dados Oracle se quiser proteger os bancos de dados Oracle.



Pré-requisitos para adicionar hosts e instalar o pacote Plug-ins para Linux ou AIX

Antes de adicionar um host e instalar os pacotes de plug-ins, você deve completar todos os requisitos.

- Se estiver a utilizar iSCSI, o serviço iSCSI tem de estar em execução.
- Você deve ter habilitado a conexão SSH baseada em senha para o usuário root ou não root.

  O plug-in do SnapCenter para banco de dados Oracle pode ser instalado por um usuário não-root. No entanto, você deve configurar o sudo Privileges para que o usuário não-root instale e inicie o processo de plug-in. Depois de instalar o plug-in, os processos serão executados como um usuário não-root eficaz.

- Se você estiver instalando o pacote de plug-ins do SnapCenter para AIX no host AIX, você deverá ter resolvido manualmente os links simbólicos no nível do diretório.

  O pacote de plug-ins do 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 o modo de autenticação como Linux ou AIX para o usuário de instalação.
- Você deve ter instalado o Java 11 em seu host Linux ou AIX.
  - Java da Oracle e OpenJDK é suportado para Linux
  - IBM Java para AIX. Você pode baixar de "IBM Semeru runtimes Downloads"

    Certifique-se de ter instalado apenas a edição certificada DO Java 11 no host Linux.

- Para bancos de dados Oracle que estão sendo executados em um host Linux ou AIX, você deve instalar o plug-in SnapCenter para banco de dados Oracle e o plug-in SnapCenter para UNIX.

Você também pode usar o Plug-in para Oracle Database para gerenciar bancos de dados Oracle para SAP. No entanto, a integração SAP BR*Tools não é suportada.

- Se você estiver usando o banco de dados Oracle 11.2.0.3 ou posterior, você deve instalar o patch 13366202 Oracle.

O mapeamento UUID no arquivo /etc/fstab não é suportado pelo SnapCenter.

- Você deve ter **bash** como o shell padrão para instalação do plug-in.

Requisitos de 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 em sistemas operacionais Oracle Linux ou Red Hat Enterprise Linux 6,6 ou 7,0, instale a versão mais recente do Logical volume Manager (LVM). • SUSE Linux Enterprise Server (SLES)
RAM mínima para o plug-in SnapCenter no host	2 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto.

Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Configure sudo Privileges 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 de plug-in serão executados como um usuário não-root eficaz. Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se o umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro devem ter permissão de 555. Caso contrário, a instalação do plug-in pode falhar.
- Para o usuário não-root, certifique-se de que o nome do usuário não-root e do grupo do usuário devem ser os mesmos.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos de código de autenticação de mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

  Reinicie o serviço sshd depois de 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 o sudo Privileges para que o usuário não-root forneça acesso aos seguintes caminhos:

- /Home/*Linux_USER*/.SC_NetApp/SnapCenter_linux_host_plugin.bin
- /Custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/SnapCenter/spl/bin/spl

Passos

1. Faça 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 !visiblepw
Defaults: LINUX_USER !requiretty
```

Se você estiver tendo uma configuração RAC, juntamente 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**, que está localizado em:

- Se o servidor SnapCenter estiver instalado no host do Windows, o SnapCenter NetApp não será instalado no sistema operacional Windows.
- */opt/NetApp/SnapCenter/SnapManagerWeb/Repository/SC_UNIX_plugins_checksum.txt* se o servidor SnapCenter estiver instalado no host Linux.

O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Requisitos de anfitrião do AIX

Você deve garantir que o host atenda aos requisitos antes de instalar o pacote de plug-ins do SnapCenter para AIX.

O plug-in do SnapCenter para UNIX, que faz parte do pacote de plug-ins do SnapCenter para AIX, não suporta grupos de volume 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 log para o plug-in SnapCenter no host	2 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto.

Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Configure sudo Privileges para usuários não-root para host AIX

O SnapCenter 4,4 e posterior permite que um usuário não root instale o pacote de plug-ins do SnapCenter para AIX e inicie o processo de plug-in. Os processos de plug-in serão executados como um usuário não-root eficaz. Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se o umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro devem ter permissão de 555. Caso contrário, a instalação do plug-in pode falhar.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos de código de autenticação de mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

  Reinicie o serviço sshd depois de 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 o sudo Privileges para que o usuário não-root forneça acesso aos seguintes caminhos:

- /Home/*AIX_USER*/.SC_NetApp/SnapCenter_aix_host_plugin.bsx

- /Custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/SnapCenter/spl/bin/spl

Passos

1. Faça 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: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

Se você estiver tendo uma configuração RAC, juntamente 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**, que está localizado em:

- Se o servidor SnapCenter estiver instalado no host do Windows, o SnapCenter NetApp não será instalado no sistema operacional Windows.
- */opt/NetApp/SnapCenter/SnapManagerWeb/Repository/SC_UNIX_plugins_checksum.txt* se o servidor SnapCenter 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 plug-in em hosts Linux ou AIX.

Sobre esta tarefa

As credenciais são criadas para o usuário raiz ou para um usuário não-root que tenha sudo Privileges para instalar e iniciar o processo de plug-in.

Para obter informações, consulte: Configure sudo Privileges para usuários não-root para host Linux Ou Configure sudo Privileges para usuários não-root para host AIX

Prática recomendada: embora você tenha permissão para criar credenciais após implantar hosts e instalar plug-ins, a prática recomendada é criar credenciais após 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 **Credential**.
3. Clique em **novo**.
4. Na página Credential (credencial), insira as informações da credencial:

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para as credenciais.
Nome de utilizador/Palavra-passe	Introduza o nome de utilizador e a palavra-passe a utilizar para a autenticação. • Administrador de domínio Especifique o administrador de domínio no 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 (apenas para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é: *Nome de usuário*

Para este campo…	Faça isso…
Modo de autenticação	Selecione o modo de autenticação que pretende utilizar. Dependendo do sistema operacional do host plug-in, selecione Linux ou AIX.
Use sudo Privileges	Marque a caixa de seleção **Use sudo Privileges** se estiver criando credenciais para um usuário que não seja root.

5. Clique em **OK**.

Depois de concluir a configuração das credenciais, você pode querer 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 usadas para executar operações de proteção de dados em bancos de dados Oracle.

Sobre esta tarefa

Você deve rever os diferentes métodos de autenticação suportados para o banco de dados Oracle. Para obter informações, "Métodos de autenticação para suas credenciais"consulte .

Se você configurar credenciais para grupos de recursos individuais e o nome de usuário não tiver Privileges de administrador completo, o nome de usuário deve ter, pelo menos, Privileges de grupo de recursos e backup.

Se você ativou a autenticação do banco de dados Oracle, um ícone de cadeado vermelho será exibido na exibição recursos. Você deve configurar credenciais de 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 durante a criação de 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 **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** na lista **Exibir**.
3. Clique em e selecione o nome do host e o tipo de banco de dados para filtrar os recursos.

   Em seguida, pode 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 configurações do banco de dados, na lista suspensa **usar credencial existente**, selecione a credencial que deve ser usada para executar tarefas de proteção de dados no banco de dados Oracle.

O usuário Oracle deve ter sysdba Privileges.

Você também pode criar uma credencial clicando em .

6. Na seção Configurar configurações ASM, na lista suspensa **usar credencial existente**, selecione a credencial que deve ser usada para executar tarefas de proteção de dados na instância ASM.

   O usuário ASM deve ter privilégio sysasm.

   Você também pode criar uma credencial clicando em .

7. Na seção Configurar configurações do catálogo RMAN, na lista suspensa **usar credencial existente**, selecione a credencial que deve ser usada para executar tarefas de proteção de dados no banco de dados de catálogo do Oracle Recovery Manager (RMAN).

   Você também pode criar uma credencial clicando em .

   No campo **TNSName**, insira o nome do arquivo do substrato de rede transparente (TNS) que será usado pelo servidor SnapCenter para se comunicar com o banco de dados.

8. No campo **Preferred RAC Nodes**, especifique os nós do Real Application Cluster (RAC) preferidos para backup.

   Os nós preferidos podem ser um ou todos os nós de cluster onde as instâncias de 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 preferido é o nó onde o banco de dados está hospedado atualmente.

   Após o failover ou realocação do banco de dados RAC de um nó, a atualização de recursos na página recursos do SnapCenter removerá o host da lista **Preferred RAC Nodes**, onde o banco de dados foi hospedado anteriormente. O nó RAC onde o banco de dados é realocado será listado em **nós RAC** e precisará ser configurado manualmente como o nó RAC preferido.

   Para obter mais informações, "Nós preferenciais na configuração RAC"consulte .

9. Clique em **OK**.

Adicione hosts e instale o pacote Plug-ins para Linux ou AIX usando GUI

Você pode usar a página Adicionar host para adicionar hosts e, em seguida, instalar o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do 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 Oracle RAC One Node, você deve instalar o plug-in em nós ativos e passivos.

Somente a autenticação baseada em senha é suportada quando você estiver instalando o plug-in em um Oracle RAC. A autenticação baseada em chave SSH não é suportada.

Você deve ser atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.

Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Verifique se a guia **hosts gerenciados** está selecionada na parte superior.
3. Clique em **Add**.
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 servidor SnapCenter adiciona o host e, em seguida, instala o plug-in para banco de dados Oracle e o plug-in para UNIX se os plug-ins ainda não estiverem instalados no host.
Nome do host	Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no FQDN. Você pode inserir os endereços IP ou FQDN de um dos seguintes: • Anfitrião independente • Qualquer nó no ambiente do Oracle Real Application clusters (RAC) O nó VIP ou IP de digitalização não é suportado 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 exibir 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 instalar.
6. (Opcional) clique em **mais opções**.

Para este campo…	Faça isso…
Porta	Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido 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, você deve especificar a mesma porta. Caso contrário, a operação falha.
Caminho de instalação	O caminho padrão é */opt/NetApp/SnapCenter*. Opcionalmente, você pode personalizar o caminho.
Adicione todos os hosts no Oracle RAC	Marque essa caixa de seleção para adicionar todos os nós de cluster em um Oracle RAC. Em uma configuração do Flex ASM, todos os nós, independentemente de ser um nó Hub ou Leaf, serão adicionados.

Para este campo…	Faça isso…
Ignorar verificações de pré-instalação opcionais	Marque essa 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 selecionado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar 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 for especificado nas regras de rejeição do firewall.

   Mensagens de erro ou aviso apropriadas são 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: SnapCenter NetApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, será necessário atualizar o arquivo em ambos os nós.

8. Verifique a impressão digital e clique em **Confirm and Submit**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós no cluster.

   O SnapCenter não suporta o algoritmo ECDSA.

   A verificação de impressões digitais é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitorize 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 automaticamente descobertos e exibidos na página recursos. Se nada for exibido, clique em **Atualizar recursos**.

Monitorar o status da instalação

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso

- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
   a. Clique em **filtro**.
   b. Opcional: Especifique a data de início e fim.
   c. No menu suspenso tipo, selecione **Instalação 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 **Visualizar logs**.

Maneiras alternativas de instalar o pacote Plug-ins para Linux ou AIX

Você também pode instalar o pacote 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** localizada em *C:\ProgramData\NetApp\SnapCenter Package\Repository*.

Certifique-se de que **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 o host AIX: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bsx.sig snapcenter_linux_host_plugin.bsx`

Instale em vários hosts remotos usando cmdlets

Você deve usar o cmdlet *Install-SmHostPackage* 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 conetado 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 servidor SnapCenter, estabeleça uma sessão usando o cmdlet *Open-SmConnection* e insira suas credenciais.
3. Instale o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do 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 for 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Instalar no host do cluster

Você deve instalar o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter 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 respetivos nós e o segundo IP será o IP do cluster compartilhado entre ambos os nós.

Passos

1. Instale o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX nos dois nós do host do cluster.
2. Valide que os valores corretos para os parâmetros SnapCenter_SERVER_HOST, SPL_PORT, SnapCenter_SERVER_PORT e SPL_ENABLED_PLUGINS são especificados no arquivo spl.properties localizado em */var/opt/SnapCenter/spl/etc/*.

   Se SPL_ENABLED_PLUGINS não for especificado no spl.properties, você pode adicioná-lo e atribuir o valor SCO,SCU.

3. No host do servidor SnapCenter, estabeleça uma sessão usando o cmdlet *Open-SmConnection* e insira suas credenciais.
4. Em cada um dos nós, defina os IPs preferidos do nó usando o comando *set-PreferredHostIPsInStorageExportPolicy* sccli e os parâmetros necessários.
5. No host do servidor SnapCenter, 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 servidor SnapCenter 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 quaisquer outras operações do SnapCenter estiverem em execução.

Instale o pacote Plug-ins para Linux no modo silencioso

Você pode instalar o pacote de plug-ins do SnapCenter para Linux no modo silencioso usando a interface de linha de comando (CLI).

O que você vai precisar

- Você deve rever os pré-requisitos para instalar o pacote de plug-ins.
- Você deve garantir que a variável de ambiente de EXIBIÇÃO não esteja definida.

  Se a variável de ambiente DE EXIBIÇÃO estiver definida, você deverá executar A EXIBIÇÃO não definida e, em seguida, tentar instalar manualmente o plug-in.

Sobre esta tarefa

Você é obrigado a fornecer as informações de instalação necessárias durante a instalação no modo console, enquanto na instalação do modo silencioso você não precisa fornecer nenhuma informação de instalação.

Passos

1. Faça o download do pacote de plug-ins do SnapCenter para Linux a partir do local de instalação do servidor SnapCenter.

   O caminho de instalação padrão é *C:/ProgramData/NetApp/SnapCenter/PackageRepository*. Este caminho é acessível a partir do host onde o servidor SnapCenter está instalado.

2. No prompt de comando, navegue até o diretório onde você baixou o arquivo de instalação.
3. Executar

   ```
   ./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, em seguida, reinicie o serviço SnapCenter Plug-in Loader.

A instalação do pacote plug-ins Registra os plug-ins no host e não no servidor SnapCenter. Você deve Registrar os plug-ins no servidor SnapCenter adicionando o host usando a GUI do SnapCenter ou cmdlet do PowerShell. Ao adicionar o host, selecione "nenhum" como a credencial. Depois que o host é adicionado, os plug-ins instalados são descobertos automaticamente.

Instale o pacote Plug-ins para AIX no modo silencioso

Você pode instalar o pacote de plug-ins do SnapCenter para AIX no modo silencioso usando a interface de linha de comando (CLI).

O que você vai precisar

- Você deve rever os pré-requisitos para instalar o pacote de plug-ins.
- Você deve garantir que a variável de ambiente de EXIBIÇÃO não esteja definida.

  Se a variável de ambiente DE EXIBIÇÃO estiver definida, você deverá executar A EXIBIÇÃO não definida e, em seguida, tentar instalar manualmente o plug-in.

Passos

1. Faça o download do pacote de plug-ins do SnapCenter para AIX a partir do local de instalação do servidor SnapCenter.

   O caminho de instalação padrão é *C:/ProgramData/NetApp/SnapCenter/PackageRepository*. Este caminho é acessível a partir do host onde o servidor SnapCenter está instalado.

2. No prompt de comando, navegue até o diretório onde você baixou o arquivo de instalação.
3. Executar

   ```
   ./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, em seguida, reinicie o serviço SnapCenter Plug-in Loader.

> A instalação do pacote plug-ins Registra os plug-ins no host e não no servidor SnapCenter. Você deve Registrar os plug-ins no servidor SnapCenter adicionando o host usando a GUI do SnapCenter ou cmdlet do PowerShell. Ao adicionar o host, selecione "nenhum" como a credencial. Depois que o host é adicionado, os plug-ins instalados são descobertos automaticamente.

Configure o serviço SnapCenter Plug-in Loader

O serviço SnapCenter Plug-in Loader carrega o pacote plug-in para Linux ou AIX para interagir com o servidor SnapCenter. O serviço Plug-in Loader do SnapCenter é instalado quando você instala o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX.

Sobre esta tarefa

Depois de instalar o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX, o serviço Loader do plug-in do SnapCenter é iniciado automaticamente. Se o serviço Loader de plug-in do SnapCenter não for iniciado automaticamente, você deve:

- Certifique-se de que o diretório em que o plug-in está a funcionar não é eliminado
- Aumente o espaço de memória atribuído à Máquina Virtual Java

O arquivo spl.properties, que está localizado em */custom_location/NetApp/SnapCenter/spl/etc/*, contém os seguintes parâmetros. Os valores padrão são atribuídos a esses parâmetros.

Nome do parâmetro	Descrição
LOG_LEVEL	Apresenta os níveis de registo suportados. Os valores possíveis são TRACE, DEBUG, INFO, WARN, ERROR e FATAL.
SPL_PROTOCOL (PROTOCOLO SPL)	Apresenta o protocolo suportado pelo Plug-in Loader SnapCenter. Apenas o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver ausente.
SnapCenter_SERVER_PROTOCOL	Apresenta o protocolo suportado pelo servidor SnapCenter. Apenas o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver ausente.
SKIP_JAVAHOME_UPDATE	Por padrão, o serviço SPL deteta o caminho java e atualiza o parâmetro Java_HOME. Portanto, o valor padrão é definido como FALSE. Você pode definir como VERDADEIRO se quiser desativar o comportamento padrão e corrigir manualmente o caminho java.
SPL_KEYSTORE_PASS	Exibe a senha do arquivo keystore. Você pode alterar esse valor somente se você alterar a senha ou criar um novo arquivo de keystore.
SPL_PORT	Exibe o número da porta na qual o serviço Plug-in Loader do SnapCenter está sendo executado. Você pode adicionar o valor se o valor padrão estiver ausente. Você não deve alterar o valor depois de instalar os plug-ins.
SnapCenter_Server_HOST	Exibe o endereço IP ou o nome do host do servidor SnapCenter.
SPL_KEYSTORE_PATH	Exibe o caminho absoluto do arquivo keystore.
SnapCenter_SERVER_PORT	Exibe o número da porta na qual o servidor SnapCenter está sendo executado.

Nome do parâmetro	Descrição
REGISTOS_MAX_COUNT	Exibe o número de arquivos de log do Loader do plug-in do SnapCenter que são retidos na pasta */custom_location/SnapCenter/spl/logs*. O valor padrão é definido como 5000. Se a contagem for superior ao 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 Loader Plug-in SnapCenter 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 da inicialização do SPL.
LOG_MAX_SIZE	Apresenta o tamanho máximo do ficheiro de registo de trabalhos. Assim que o tamanho máximo for atingido, o ficheiro de registo é zipado e os registos são gravados no novo ficheiro desse trabalho.
RETER_LOGS_OF_LAST_DAYS	Exibe o número de dias até os quais os logs são mantidos.
ENABLE_CERTIFICATE_VALIDATION	Exibe verdadeiro quando a validação do certificado CA está ativada para o host. Você pode ativar ou desativar esse parâmetro editando o spl.properties ou usando a GUI ou cmdlet do SnapCenter.

Se algum destes parâmetros não estiver atribuído ao valor predefinido ou se pretender atribuir ou alterar o valor, pode modificar o ficheiro spl.properties. Você também pode verificar o arquivo spl.properties e editar o arquivo 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 um 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 um usuário não-root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

> Você pode usar a opção -force com o comando stop para parar o serviço SnapCenter Plug-in Loader com força. No entanto, você deve ter cuidado antes de fazê-lo, porque ele também termina as operações existentes.

◦ Reinicie o serviço SnapCenter Plug-in Loader:

- Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
- Como um 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 um 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 um usuário não-root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configure o 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 armazenamento de confiança SPL e configurar o par de chaves assinadas CA para o armazenamento de confiança 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', tanto como seu armazenamento de confiança e armazenamento de chaves.

Gerenciar senha para o armazenamento de chaves SPL e alias do par de chaves assinadas CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore SPL do arquivo de propriedade SPL.

É o valor correspondente à chave 'SPL_KEYSTORE_PASS'.

2. Altere a senha do keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Altere a senha para 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 depois de alterar a senha.

A senha para o keystore SPL e para todos os alias associados da chave privada deve ser a mesma.

Configure certificados raiz ou intermediários para o armazenamento de confiança SPL

Você deve configurar os certificados raiz ou intermediários sem a chave privada para o armazenamento de confiança SPL.

Passos

1. Navegue até a pasta que contém o keystore SPL: */var/opt/SnapCenter/spl/etc*.
2. Localize o arquivo 'keystore.jks'.
3. Liste 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 depois de configurar os certificados raiz ou
intermédios para o armazenamento de confiança SPL.
```

Você deve adicionar o certificado de CA raiz e, em seguida, os certificados de CA intermediários.

Configure o par de chaves assinadas da CA para o armazenamento de confiança SPL

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança SPL.

Passos

1. Navegue até a pasta que contém o keystore /var/opt/SnapCenter/spl/etc. do SPL
2. Localize o arquivo 'keystore.jks'.
3. Liste 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
. Liste os certificados adicionados no keystore.
```

```
 keytool -list -v -keystore keystore.jks
. Verifique se o keystore contém o alias correspondente ao novo
certificado da CA, que foi adicionado ao keystore.
. Altere a senha da chave privada adicionada para o certificado da 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 espaço ou
carateres especiais ("*",","), altere o nome do alias para um nome
simples:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configure o nome do alias a partir do keystore localizado no arquivo
spl.properties.
```

Atualize este valor com a chave SPL_CERTIFICATE_ALIAS.

4. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança SPL.

Configurar a lista de revogação de certificados (CRL) para SPL

Você deve configurar a CRL para SPL

Sobre esta tarefa

- O SPL procurará os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL para SPL é */var/opt/SnapCenter/spl/etc/crl*.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo spl.properties contra 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.

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet RUN *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando as *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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- * * Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da 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 são concluídas com êxito.

Importar dados do SnapManager para Oracle e SnapManager para SAP para SnapCenter

A importação de dados do SnapManager para Oracle e SnapManager para SAP para SnapCenter permite que você continue usando seus dados de versões anteriores.

Você pode importar dados do SnapManager para Oracle e SnapManager para SAP para SnapCenter executando a ferramenta de importação a partir da interface de linha de comando (CLI de 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 realizados usando esses perfis no SnapManager para Oracle e no SnapManager para SAP. A ferramenta de importação do SnapCenter interage com os bancos de dados de repositório do SnapManager para Oracle e SnapManager para SAP e o banco de dados que você deseja importar.

- Recupera todos os perfis, programações e operações realizadas 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 do SnapCenter para Linux no host de 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 suporta Data ONTAP operando no modo 7D. Você pode usar a ferramenta de transição de 7 modos para migrar dados e configurações que são 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 SnapManager 3,4.x para SAP para SnapCenter, você deve estar ciente das configurações que são suportadas com o plug-in SnapCenter para banco de dados Oracle.

As configurações compatíveis com o plug-in SnapCenter para banco de dados Oracle estão listadas na "Ferramenta de Matriz de interoperabilidade do NetApp".

O que é importado para o SnapCenter

Você pode importar perfis, programações e operações realizadas usando os perfis.

Da 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 escopo de backup como Full.

Da SnapManager para Oracle e SnapManager para SAP	Para SnapCenter
Perfis com uma ou mais operações	Várias políticas são criadas com base em uma combinação única de um perfil e operações realizadas usando esse perfil. As políticas criadas no SnapCenter contêm os detalhes de eliminação e retenção de Registros de arquivamento recuperados do perfil e das operações correspondentes.
Perfis com configuração do Oracle Recovery Manager (RMAN)	As políticas são criadas com a opção **Backup do Catálogo com o Oracle Recovery Manager** ativada. Se a catalogação RMAN externa foi usada no SnapManager, você deve configurar as configurações do catálogo RMAN no SnapCenter. Você pode selecionar a credencial existente ou criar uma nova credencial. Se o RMAN foi configurado através do arquivo de controle no SnapManager, então você não precisa configurar o RMAN no SnapCenter.
Agendamento anexado a um perfil	Uma política é criada apenas para a programação.
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 preferido após a importação e o grupo de recursos é criado para esse nó.

Quando um perfil é importado, uma política de verificação é criada juntamente com a política de backup.

Quando os perfis SnapManager for Oracle e SnapManager for SAP, os horários e quaisquer operações realizadas usando os perfis são importados para o SnapCenter, os diferentes valores de parâmetros também são importados.

SnapManager para Oracle e SnapManager para SAP parâmetros e valores	Parâmetros e valores do SnapCenter	Notas
Escopo de backup • Cheio • Dados • Registo	Escopo de backup • Cheio • Dados • Registo	
Modo de cópia de segurança • Auto • Online • Offline	Tipo de cópia de segurança • Online • Encerramento offline	Se o modo de cópia de segurança for Auto, a ferramenta de importação verifica o estado da base de dados quando a operação foi executada e define adequadamente o tipo de cópia de segurança como Desligamento Online ou Offline.
Retenção • Dias • Conta	Retenção • Dias • Conta	O SnapManager para Oracle e o SnapManager para SAP usam dias e contagens para definir a retenção. Em SnapCenter, há dias *OU* contagens. Assim, a retenção é definida em relação aos dias, à medida que os dias recebem preferência em relação às contagens no SnapManager para Oracle e no SnapManager para SAP.
Poda para horários • Tudo • Número de mudança do sistema (SCN) • Data • Logs criados antes de horas, dias, semanas e meses especificados	Poda para horários • Tudo • Registos criados antes de horas e dias especificados	A SnapCenter não suporta a poda com base no SCN, Data, semanas e meses.

SnapManager para Oracle e SnapManager para SAP parâmetros e valores	Parâmetros e valores do SnapCenter	Notas
Notificação • E-mails enviados apenas para operações bem-sucedidas • E-mails enviados apenas para operações com falha • E-mails enviados para operações de sucesso e falha	Notificação • Sempre • Falha ao ligar • 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.

Não é possível importar o seguinte para o SnapCenter:

- Metadados de backup
- Backups parciais
- Backups relacionados ao RDM (Raw Device mapping) e VSC (Virtual Storage Console)
- Funções ou quaisquer credenciais disponíveis no repositório SnapManager para Oracle e SnapManager para SAP
- Dados relacionados a operações de verificação, restauração e clone
- Poda para operações
- Detalhes de replicação especificados no perfil SnapManager para Oracle e SnapManager para SAP

  Após a importação, você deve editar manualmente a política correspondente criada no SnapCenter para incluir os detalhes da replicação.

- Informações de backup catalogadas

Prepare-se para importar dados

Antes de importar dados para o SnapCenter, é necessário executar determinadas tarefas para executar a operação de importação com êxito.

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 **Resources** e selecione o plug-in apropriado na lista.
5. Na página recursos, verifique se o banco de dados a ser importado é descoberto e exibido.

Quando você deseja executar a ferramenta de importação, o banco de dados deve estar acessível ou então a criação do grupo de recursos falha.

Se o banco de dados tiver credenciais configuradas, você deverá criar uma credencial correspondente no SnapCenter, atribuir a credencial ao banco de dados e executar novamente a descoberta do banco de dados. Se o banco de dados estiver residindo no Gerenciamento Automático de armazenamento (ASM), você deverá criar credenciais para a instância ASM e atribuir a credencial ao banco de dados.

6. Certifique-se de que o usuário que executa a ferramenta de importação tenha Privileges suficiente para executar os comandos SnapManager para Oracle ou SnapManager para SAP CLI (como o comando para suspender programações) do SnapManager para Oracle ou SnapManager para host SAP.
7. Execute os seguintes comandos no host SnapManager para Oracle ou SnapManager para SAP para suspender as programações:
   a. Se você quiser suspender as programações no host SnapManager para 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 as programações no host SnapManager for 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 deverá 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 diferentes formatos de nomenclatura:

- As políticas criadas para os perfis sem nenhuma operação e programação 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 on-line e o escopo de backup como cheio.

- As políticas criadas para os perfis com uma ou mais operações têm o formato SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED.
- As políticas criadas para as programações anexadas aos perfis têm o formato SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED.

Passos

1. Faça 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. Introduza o nome de utilizador e a palavra-passe do servidor SnapCenter.

   Depois de 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. Introduza os detalhes da base de dados de destino.

   Se você quiser importar todos os bancos de dados no host, insira todos.

6. Se você deseja gerar um log do sistema ou enviar mensagens ASUP para operações com falha, você deve ativá-las executando o comando *Add-SmStorageConnection* ou *set-SmStorageConnection*.

> Se você quiser cancelar uma operação de importação, seja durante a execução da ferramenta de importação ou após a importação, exclua 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, programações e operações executadas usando os perfis. Os grupos de recursos também são criados para cada banco de dados de destino.

Depois de importar os dados com êxito, as programações associadas ao banco de dados importado são suspensas no SnapManager para Oracle e no SnapManager para SAP.

> Após a importação, você deve gerenciar o banco de dados importado ou o sistema de arquivos usando o SnapCenter.

Os logs para 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.

Instale o plug-in do SnapCenter para VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs) ou se você quiser proteger VMs e datastores, você deverá implantar o plug-in do SnapCenter para o dispositivo virtual VMware vSphere.

Para obter informações sobre como implantar, "Visão geral da implantação" consulte .

Implantar certificado CA

Para configurar o certificado CA com o plug-in SnapCenter para VMware vSphere, "Criar ou importar certificado SSL" consulte .

Configure o arquivo CRL

O plug-in do SnapCenter para VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL para o plug-in do SnapCenter para 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, clone ou restauração, você precisa definir sua estratégia e configurar o ambiente. Você também pode configurar o servidor SnapCenter para usar a tecnologia SnapMirror e SnapVault.

Para aproveitar as tecnologias SnapVault e SnapMirror, você deve configurar e inicializar uma relação 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 banco de dados Oracle, o administrador do SnapCenter deve instalar e configurar o servidor SnapCenter e executar as tarefas de pré-requisito.

- Instalar e configurar o servidor SnapCenter. "Saiba mais"
- Configure o ambiente SnapCenter adicionando conexões do sistema de storage. "Saiba mais"

> O SnapCenter não é compatível com vários SVMs com o mesmo nome em clusters diferentes. Cada SVM registrado no SnapCenter usando o Registro da SVM ou o Registro de cluster precisa ser único.

- Crie credenciais com o modo de autenticação como Linux ou AIX para o usuário de instalação. "Saiba mais"
- Adicione hosts, instale os plug-ins e descubra os recursos.
- Se você estiver usando o servidor SnapCenter para proteger bancos de dados Oracle que residem em LUNs ou VMDKs do VMware RDM, será necessário implantar o plug-in do SnapCenter para VMware vSphere e Registrar o plug-in com o SnapCenter.

- Instale o Java em seu host Linux ou AIX.

  "Requisitos de host do Linux"Consulte ou "Requisitos do anfitrião de AIX" para obter 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, configure pelo menos um LIF de dados NFS para storage primário ou secundário para executar operações de montagem, clone, verificação e restauração.
- Se você tiver vários caminhos de dados (LIFs) ou uma configuração DNFS, você pode 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 storage NFS na máquina virtual de armazenamento (SVM) para os volumes clonados. Se você quiser ter um endereço IP específico ou restringir a um subconjunto dos endereços IP, execute a CLI Set-PreferredHostIPsInStorageExportPolicy.
  - Se você tiver vários caminhos de dados (LIFs) na SVM, o SnapCenter escolherá o caminho de dados (LIF) apropriado para a montagem do volume clonado NFS. No entanto, se você quiser especificar um caminho de dados específico (LIF), você deve executar a CLI Set-SvmPreferredDataPath. O guia de referência do comando tem mais informações.
- Se você tiver bancos de dados Oracle em ambientes SAN, verifique se o ambiente SAN está configurado de acordo com a recomendação mencionada nos guias a seguir:
  - "Configurações de host recomendadas para utilitários de host unificado do Linux"
  - "Configurações do host afetadas pelos Utilitários de 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 plug-in do SnapCenter para o banco de dados Oracle, é possível 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 você quiser replicação de backup

Para usuários do SnapCenter 4.1.1, a documentação do plug-in do SnapCenter para VMware vSphere 4.1.1 tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos. Para usuários do SnapCenter 4,2.x, o Agente de dados do NetApp 1,0 e 1,0.1, a documentação tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in do SnapCenter para 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 plug-in do SnapCenter para VMware vSphere 4,3 tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in SnapCenter baseado no Linux para o dispositivo virtual VMware vSphere (formato Open Virtual Appliance).

Encontre mais informações

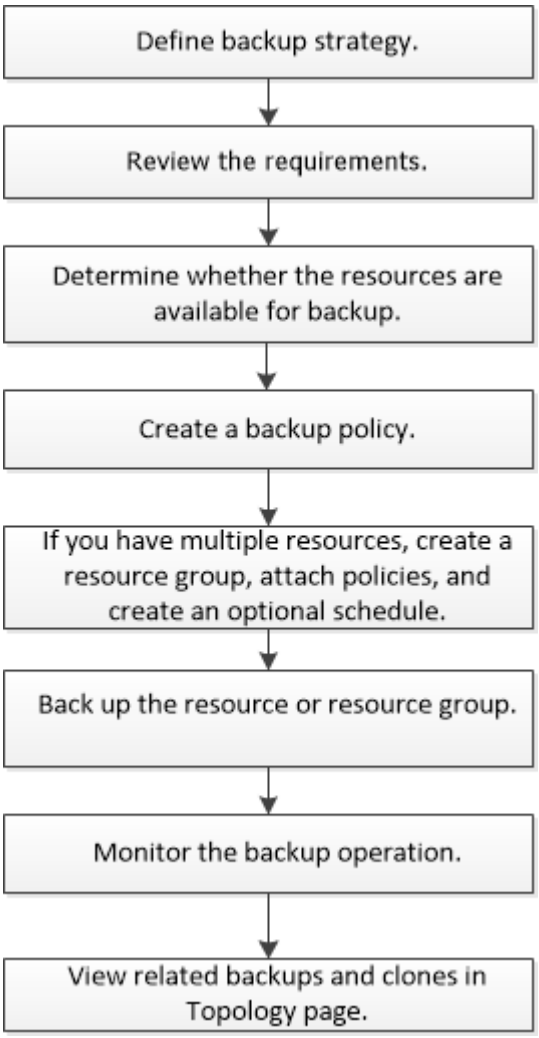
- "Ferramenta de Matriz de interoperabilidade"
- "Plug-in do SnapCenter para documentação do VMware vSphere"
- "Falha na operação de proteção de dados em um ambiente não multipath no RHEL 7 e posterior"

Faça 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 inclusão 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 de 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.

No entanto, 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 para */var/opt/SnapCenter/SCO/lock*.
2. Eliminar o bloqueio operacional:`rm -rf .sm_lock_dbsid.`

Informações de configuração de backup

Configurações de banco de dados Oracle compatíveis para backups

O SnapCenter suporta backup de diferentes configurações de banco de dados Oracle.

- Oracle Standalone
- Oracle Real Application clusters (RAC)
- Oracle Standalone Legacy
- Oracle Standalone Container Database (CDB)
- Espera do Oracle Data Guard

  Você só pode criar backups de montagem offline de bancos de dados em espera do Data Guard. Backup off-line-shutdown, backup somente de log de arquivamento e backup completo não são suportados.

- Espera do Oracle ative Data Guard

  Você só pode criar backups online de bancos de dados em espera do ative Data Guard. O backup e o backup completo somente de log de arquivamento não são suportados.

  Antes de criar um backup do banco de dados de espera do Data Guard ou do ative Data Guard, o processo de recuperação gerenciado (MRP) é interrompido e, uma vez que o backup é criado, o MRP é iniciado.

- Gerenciamento automático de storage (ASM)
  - ASM autônomo e ASM RAC no Virtual Machine Disk (VMDK)

    Entre todos os métodos de restauração suportados para bancos de dados Oracle, você pode executar apenas a restauração de conexão e cópia de bancos de dados ASM RAC no VMDK.

  - ASM autônomo e ASM RAC em mapeamento de dispositivo bruto (RDM), você pode executar operações de backup, restauração e clone em bancos de dados Oracle no ASM, com ou sem ASMLib.
  - Controlador de filtro Oracle ASM (ASMFD)

    As operações de migração PDB e clonagem PDB não são suportadas.

  - Oracle Flex ASM

Para obter as informações mais recentes sobre versões Oracle suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Tipos de backup suportados para bancos de dados Oracle

Tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter suporta tipos de backup on-line e off-line para bancos de dados Oracle.

Backup on-line

Um backup que é criado quando o banco de dados está no estado on-line é chamado de backup on-line. Também chamado de hot backup, um backup on-line permite que você crie um backup do banco de dados sem desligá-lo.

Como parte do backup on-line, você pode criar um backup dos seguintes arquivos:

- Arquivos de dados e arquivos de controle somente
- Arquivar apenas ficheiros de registo (a base de dados não é colocada no modo de cópia de segurança neste cenário)
- Banco de dados completo que inclui arquivos de dados, arquivos de controle e arquivos de log de arquivamento

Cópia de segurança offline

Um backup criado quando o banco de dados está em um estado montado ou desligado é chamado de backup off-line. Um backup off-line também é chamado de backup frio. Você pode incluir somente arquivos de dados e arquivos de controle em backups offline. Você pode criar um backup de montagem off-line ou de desligamento off-line.

- Ao criar um backup de montagem off-line, 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 off-line, o banco de dados pode estar em qualquer estado.

  O estado da base de dados é alterado para o estado necessário para criar uma cópia de segurança. Depois de criar a cópia de segurança, o estado da base 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

Base 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 autônomos são descobertos apenas com base em entradas /etc/oratab.

ASM

A entrada de instância ASM deve estar disponível no arquivo /etc/oratab.

Nó RAC um

Os bancos de dados RAC One Node são descobertos apenas com base em entradas /etc/oratab. Os bancos de dados devem estar em nomount, mount ou em estado aberto. Você deve ter as entradas do banco de dados no arquivo /etc/oratab.

O status do banco de dados RAC One Node será marcado como renomeado ou excluído se o banco de

dados já estiver descoberto e os backups estiverem 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 realocada no arquivo /etc/oratab no nó RAC com falha.
2. Atualizar 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 preferidos para o nó RAC que hospeda o banco de dados atualmente.
5. Execute as operações do SnapCenter.
6. Se você tiver relocado um banco de dados de um nó para outro nó 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

Base 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 autônomos são descobertos com base nas entradas no arquivo /etc/oratab e na saída do comando srvctl config.

ASM

A entrada de instância ASM não precisa estar no arquivo /etc/oratab.

Nó RAC um

Os bancos de dados RAC One Node são descobertos usando apenas o comando srvctl config. Os bancos de dados devem estar em nomount, mount ou em estado aberto. O status do banco de dados RAC One Node será marcado como renomeado ou excluído se o banco de dados já estiver descoberto e os backups estiverem associados ao banco de dados.

Você deve executar as seguintes etapas se o banco de dados for realocado: . Atualizar 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 preferidos para o nó RAC que hospeda o banco de dados atualmente. . Execute as operações do SnapCenter.

> Se houver alguma entrada de banco de dados Oracle 12*c*R2 e 18*c*_ no arquivo /etc/oratab e o mesmo banco de dados estiver registrado com o comando srvctl config, o SnapCenter eliminará as entradas duplicadas do banco de dados. Se houver entradas de banco de dados obsoletas, o banco de dados será descoberto, mas o banco de dados será inacessível e o status será off-line.

Nós preferenciais na configuração RAC

Na configuração RAC (Real Application clusters) do Oracle, você pode especificar os nós preferenciais que o SnapCenter usa para executar a operação de backup. Se você não

especificar o nó preferido, o SnapCenter atribuirá automaticamente um nó como o nó preferido e o backup será criado nesse nó.

Os nós preferidos podem ser um ou todos os nós de cluster onde as instâncias de banco de dados RAC estão presentes. A operação de backup é acionada somente nesses nós preferenciais na ordem da preferência.

Exemplo

O banco de dados RAC cdbrac tem três instâncias: cdbrac1 em node1, cdbrac2 em node2 e cdbrac3 em node3.

As instâncias node1 e node2 são configuradas para serem os nós preferidos, com node2 como a primeira preferência e node1 como a segunda preferência. Quando você executa uma operação de backup, a operação é tentada pela primeira vez no node2 porque é o primeiro nó preferido.

Se o node2 não estiver no estado para fazer backup, o que pode ser devido a vários motivos, como o agente plug-in não está sendo executado no host, a instância do banco de dados no host não está no estado necessário para o tipo de backup especificado, ou a instância do banco de dados no node2 em uma configuração FlexASM não está sendo servida pela instância local ASM; então 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 Leaf Nodes não serão listados como nós preferenciais se a cardinalidade for menor que os nós numéricos no cluster RAC. Se houver alguma alteração nas funções de nó de cluster do Flex ASM, você deverá descobrir manualmente para que os nós preferidos sejam atualizados.

Estado da base 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 êxito:

- Uma das instâncias do banco de dados RAC nos nós preferenciais configurados deve estar no estado aberto para criar um backup on-line.
- 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 inferiores para criar um backup de montagem off-line.
- As instâncias de banco de dados RAC podem estar em qualquer estado, mas você deve especificar os nós preferenciais para criar um backup de desligamento off-line.

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 de ponto no tempo de tablespace. Quando você não precisa desses backups catalogados, você pode remover as informações do catálogo.

O banco de dados deve estar em estado montado ou superior para catalogação. Você pode fazer catalogação em backups de dados, backups de log de arquivamento e backups completos. Se a catalogação estiver

ativada para um backup de um grupo de recursos que tenha vários bancos de dados, a catalogação é realizada para cada banco de dados. Para bancos de dados Oracle RAC, a catalogação será realizada no nó preferido onde o banco de dados está, pelo menos, no estado montado.

Se você quiser catalogar backups de um banco de dados RAC, verifique se nenhum outro trabalho está sendo executado para esse banco de dados. Se outro trabalho estiver em execução, a operação de catalogação falhará em vez de ficar na fila.

Banco de dados de catálogo externo

Por padrão, o arquivo de controle de banco de dados de destino é usado para catalogação. Se você quiser adicionar um banco de dados de catálogo externo, você pode configurá-lo especificando o nome do substrato de rede transparente (TNS) e credencial do catálogo externo usando o assistente Configurações de banco de dados da interface gráfica do usuário (GUI) do SnapCenter. Você também pode configurar o banco de dados de catálogo externo da CLI executando o comando Configure-SmOracleDatabase com as opções -OracleRmanCatalogCredentialName e -OracleRmanCatalogTnsName.

Comando RMAN

Se você ativou a opção catalogação ao criar uma política de backup Oracle a partir da GUI do SnapCenter, os backups serão catalogados usando o Oracle RMAN como parte da operação de backup. Você também pode executar a catalogação diferida de backups executando o `Catalog-SmBackupWithOracleRMAN` comando.

Depois de catalogar os backups, você pode executar o `Get-SmBackupDetails` comando para obter as informações de backup catalogadas, como a tag para datafiles 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 carateres, a partir do SnapCenter 3,0, o formato de nomenclatura usado para o backup é SC_HASHCODEofDISKGROUP_DBSID_BACKUPID. No entanto, se o nome do grupo de discos for inferior a 16 carateres, o formato de nomenclatura usado para o backup é 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 do repositório RMAN desatualizadas sobre backups cujos Registros do 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 indica que os logs estão no disco, quando na verdade eles não estão.

A operação de verificação cruzada permite-lhe atualizar o ficheiro de controlo com as informações. Você pode ativar a verificação cruzada executando o comando Set-SmConfigSettings e atribuindo o valor TRUE ao parâmetro ENABLE_CROSSCHECK. O valor padrão é definido como FALSE.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

Remova as 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 ao excluir o backup ou ao excluir o grupo de retenção e recursos associado ao backup catalogado.

> Quando você força uma 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 deve 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"
```

Depois de 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. Em alternativa, pode consultar a "Guia de Referência de comandos do software SnapCenter".

Variáveis de ambiente predefinidas para prescrição específica de backup e postscript

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript ao criar políticas de cópia de segurança. Essa funcionalidade é compatível com todas as configurações Oracle, exceto VMDK.

O SnapCenter predefine os valores dos parâmetros que serão diretamente acessíveis no ambiente onde os scripts shell são executados. Você não precisa especificar manualmente os valores desses parâmetros ao executar os scripts.

Variáveis de ambiente predefinidas suportadas para a criação de política de backup

- **SC_JOB_ID** especifica a ID da tarefa 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 banco de dados separados por pipe.

  Esse 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 é executado.

  Esse 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 em oracle|NFSB32 em oracle

- **SC_os_GROUP** especifica o grupo do sistema operacional do banco de dados.

  Os dados serão formatados como <db1> <osgroup1>|<db2> <osgroup2>.

  Exemplo: NFSB31 a instalar|NFSB32 a instalar

- **SC_BACKUP_TYPE**" especifica o tipo de backup (dados on-line completos, on-line, log on-line, desligamento off-line, montagem off-line)

  Exemplos:

  - Para backup completo: ONLINEFULL
  - Backup apenas de dados: ONLINEDATA
  - Para backup somente de log: ONLINELOG

- **SC_BACKUP_NAME** especifica o nome do backup.

  Esse 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 de backup.

  Esse parâmetro será preenchido para volumes de aplicativos.

  EXEMPLO: DADOS EM 203|LOG EM 205|AV EM 207

- **SC_ORACLE_HOME** especifica o caminho do diretório inicial do Oracle.

  Exemplo: NFSB32/ora01/app/oracle/PRODUCT/18,1.0/dB_1|NFSB31at/ora01/app/oracle/PRODUCT/18,1.0/dB_1

- **SC_BACKUP_RETENSION** especifica o período de retenção definido na política.

  Exemplos:

  - Para backup completo: Por hora|DADOS em DIA:3|LOG em CONTAGEM:4
  - Para backup apenas de dados sob demanda: OnDemand|DATA em CONTAGEM:2
  - Para backup somente de log sob demanda: OnDemand|LOG at 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 da aplicação.

  Exemplo: AV1|AV2

- **SC_PRIMARY_DATA_VOLUME_full_PATH** especifica o mapeamento de armazenamento de SVM para o 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 bancos de dados 2 no mesmo grupo de recursos: NFSB32 a buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA|NFSB31 a buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA
  - Para um único banco de dados com arquivos de dados espalhados por vários volumes: Buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_NFS

- **SC_PRIMARY_ARCHIVELOGS_VOLUME_full_PATH** especifica o mapeamento de armazenamento de SVM para o volume para o diretório de arquivos de logs. Será o nome do volume pai para luns e qtrees.

  Exemplos:

  - Para uma única instância de banco de dados: Buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
  - Para várias instâncias de banco de dados: NFSB31 a buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO|NFSB32 a buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO

- **SC_PRIMARY_full_SNAPSHOT_NAME_FOR_TAG** especifica a lista de instantâneos contendo nome do sistema de armazenamento e nome do volume.

  Exemplos:

  - Para uma única instância de banco de dados: 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 NFSB31 07 02.28.26.3973 NFSB31 07 02.28.26.3973 a buck:/vol/2021 NFSB31 RG2 21 0 RG2 21 1_NFS_CDB_02.28.26.3973 scspr2417819002 scspr2417819002 2021 scspr2417819002 scspr2417819002 2021_DATA/21_scspr2417819002_07-RG2-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/21_scspr2417819002_07_RG2_scspr2417819002_NFSB32_1

- **SC_PRIMARY_SNAPSHOT_NAMES** especifica os nomes dos snapshots primários criados durante o backup.

  Exemplos:

  - Para instância de banco de dados único: 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_0_1|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_02.28.26.3973,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

- Para instantâneos de grupo de consistência que envolvem volumes:_R80404CBEF5V1_-05-2021_03.08.03.4945_2_cg3-28ad-465c-9d60-5487ac17b25d_2021_04_0_bfc279cc_8_58_350_4_5_3

- **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 em 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 uma única instância de banco de dados: /Mnt/nfsdb3_data,/mnt/nfsdb3_log,/mnt/nfsdb3_data1
  - Para várias instâncias de banco de dados: NFSB31at/mnt/nfsdb31_data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1|NFSB32at/mnt/nfsdb32_data,/mnt/nfsdb32_log,/mnt/nfsdb32_data1
  - PARA ASM: DATA2DG, LOG2DG

- **SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS** especifica os nomes dos instantâneos criados durante o backup de cada um dos pontos de montagem.

  Exemplos:

  - Para uma única instância de banco de dados: RG2_scspr2417819002_07-2021-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-21_02.28.26.3973_1:/mnt/nfsb31_log
  - Para várias instâncias de banco de dados: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_07_07-scspr2417819002-2021_RG2_0:/mnt/nfsb31_log|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_data,02.28.26.3973_21_scspr2417819002-21-2021_02.28.26.3973_1:/mnt/nfsb32_log

- **SC_ARCHIVELOGS_LOCATIONS** especifica a localização do diretório de logs de arquivo.

  Os nomes dos diretórios serão o pai imediato dos arquivos de log do arquivo. Se os registos de arquivo forem colocados em mais de um local, todos os locais serão capturados. Isso também inclui os cenários FRA. Se os softlinks forem usados para o diretório, o mesmo será preenchido.

  Exemplos:

  - Para um único banco de dados em NFS: /Mnt/nfsdb2_log
  - Para vários bancos de dados em NFS e para os logs de arquivo de banco de dados NFSB31 que são colocados em dois locais diferentes: NFSB31at/mnt/nfsdb31_log1,/mnt/nfsdb31_log2|NFSB32at/mnt/nfsdb32_log
  - PARA ASM: LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15

- **SC_REDO_LOGS_LOCATIONS** especifica a localização do diretório refazer logs.

  Os nomes de diretório serão o pai imediato dos arquivos de log refazer. Se os softlinks forem usados para o diretório, o mesmo será preenchido.

  Exemplos:

- Para um único banco de dados em NFS: /Mnt/nfsdb2_data/newdb1
- Para vários bancos de dados em NFS: NFSB31 a/mnt/nfsdb31_data/newdb31|NFSB32 a/mnt/nfsdb32_data/newdb32
- PARA ASM: LOG2DG/ASMDB2/ONLINELOG

- **SC_CONTROL_FILES_LOCATIONS** especifica a localização do diretório de arquivos de controle.

  Os nomes dos diretórios serão o pai imediato dos arquivos de controle. Se os softlinks forem usados para o diretório, o mesmo será preenchido.

  Exemplos:

  - Para um único banco de dados em NFS: /Mnt/nfsdb2_data/fra/newdb1,/mnt/nfsdb2_data/newdb1
  - Para vários bancos de dados em NFS: NFSB31 a/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFSB32 a/mnt/nfsdb32_data/fra/newdb32,/mnt/nfsdb32_data/newdb32
  - PARA ASM: LOG2DG/ASMDB2/CONTROLFILE
- **SC_DATA_FILES_LOCATIONS"** especifica a localização do diretório de arquivos de dados.

  Os nomes dos diretórios serão o pai imediato dos arquivos de dados. Se os softlinks forem usados para o diretório, o mesmo será preenchido.

  Exemplos:

  - Para um único banco de dados em NFS: /Mnt/nfsdb3_data1,/mnt/nfsdb3_data/NEWDB3/datafile
  - Para vários bancos de dados em NFS: NFSB31at/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/datafile|NFSB32at/mnt/nfsdb32_data1,/mnt/nfsdb32_data/NEWDB32/datafile
  - PARA ASM: DATA2DG/ASMDB2/ARQUIVO DE DADOS, DATA2DG/ASMDB2/TEMPFILE
- **SC_SNAPSHOT_LABEL** especifica o nome dos rótulos secundários.

  Exemplos: Etiqueta horária, diária, semanal, mensal ou personalizada.

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 os dados do nome do banco de dados e para separar o valor de sua chave.

  Exemplos:

  - A buck:/vol/_NFS_CDB*DATA/*--1__02.28.26.3973,buck:/vol/scspr2417819002_NFS_CDB_2021_REDO/07_RG2_scspr2417819002_NFSB31_0_scspr2417819002_02.28.26.3973_21_07_RG2_2021_NFSB31_NFSB31_scspr2417819002_1_2021_scspr2417819002_02.28.26.3973_21_scspr2417819002_07_RG2_21_NFSB32_0_2021_02.28.26.3973_21_scspr2417819002_07_RG2_NFSB32_NFSB32_scspr2417819002
  - NFSB31 de julho de NFSB32

- **|** 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_RETENSION e SC_BACKUP_NAME.

  Exemplos:

  - DATA 203|LOG EM 205
  - HORA|DADOS EM 3|LOG EM 4
  - DATA@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 Snapshot para os parâmetros SC_PRIMARY_SNAPSHOT_NAMES e SC_PRIMARY_full_snapshot_NAME_FOR_TAG.

  Exemplo: NFSB32 a buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-RG2-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/21_scspr2417819002_07-21-2021_02.28.26.3973_1

- **,** é usado para separar o conjunto de variáveis para o mesmo banco de dados.

  Exemplo: A buck:/vol/_NFS_CDB*DATA/--,buck:/vol/_NFS_CDB*REDO/__2021_02.28.26.3973_1_scspr2417819002_07|21 buck a:/vol/scspr2417819002_NFS_CDB_NFSB31_RG2_0_2021_02.28.26.3973_07_21_scspr2417819002_NFSB31_1_RG2_scspr2417819002_NFSB31_02.28.26.3973_07_21_RG2_2021_NFSB32_0_scspr2417819002_02.28.26.3973_21_scspr2417819002_07_RG2_2021_NFSB32_NFSB32_scspr2417819002_scspr2417819002

Opções de retenção de backup

Você pode escolher o número de dias para os quais reter cópias de backup ou especificar o número de cópias de backup que deseja reter, até um máximo de ONTAP de 255 cópias. Por exemplo, sua organização pode exigir que você retenha 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 tiver sido alterado para o grupo de recursos ou recursos, os backups com o rótulo de tipo de agendamento antigo ainda poderão permanecer no sistema.

Para retenção de longo prazo de cópias de backup, você deve usar o backup SnapVault.

Fazer backup de programações

A frequência de backup (tipo de agendamento) é especificada em políticas; uma programação de backup é especificada na configuração do grupo de recursos. O fator mais crítico na determinação de uma 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 usado a cada hora, enquanto você pode fazer backup de um recurso raramente usado uma vez por dia. Outros fatores incluem a importância do recurso para a sua organização, seu Contrato de nível de Serviço (SLA) e seu objetivo de ponto de recuperação (RPO).

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. Um RPO define a estratégia para a era dos arquivos que precisam ser recuperados do storage 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 usado, não é necessário executar um backup completo mais de uma ou duas vezes por dia. Por exemplo, backups regulares de log de transações podem ser suficientes para garantir que você tenha os backups necessários. Quanto mais você fizer backup de seus bancos de dados, menos Registros de transações que o SnapCenter precisa usar no momento da restauração, o que pode resultar em operações de restauração mais rápidas.

Os programas de backup têm duas partes, como segue:

- Frequência de backup

  A frequência de backup (com que frequência os backups devem ser executados), chamada *schedule type* para alguns plug-ins, faz parte de uma configuração de política. Você pode selecionar a frequência de backup da política por hora, dia, semanal ou mensal. Se você não selecionar nenhuma dessas frequências, a política criada será uma política somente sob demanda. Você pode acessar políticas clicando em **Configurações** > **políticas**.

- Fazer backup de programações

  As agendas 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 que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas. Você pode acessar programações de grupos de recursos clicando em **recursos** > **grupos de recursos**.

Convenções de nomenclatura de backup

Você pode usar a convenção padrão de nomenclatura Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um carimbo de data/hora aos nomes de Snapshot 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 carimbo de data/hora.

Como alternativa, você pode especificar o formato do nome da captura Instantânea enquanto protege recursos ou grupos de recursos selecionando **usar formato de nome personalizado para cópia Instantânea**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do carimbo de hora é adicionado ao nome do instantâneo.

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 concluídos.

- Você deve ter criado um grupo de recursos com uma política anexada.
- Se você quiser fazer backup de um recurso que tenha uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, 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 storage (SVM) usada pelo banco de dados.
- Você deve ter verificado que todos os volumes de dados e volumes de log de arquivamento pertencentes ao banco de dados estão protegidos se a proteção secundária estiver ativada para esse banco de dados.
- Você deve ter verificado que o banco de dados que tem 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 que o comprimento do ponto de montagem do volume não excede 240 carateres.
- Você deve aumentar o valor de RESTTimeout para 86400000 ms no arquivo _C: Arquivos de programas/NetApp no host do servidor SnapCenter, se o banco de dados que está sendo feito backup for grande (tamanho em TBs).

  Ao modificar os valores, certifique-se de que não existem trabalhos em execução e reinicie o serviço SnapCenter SMCore depois de 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 servidor SnapCenter, adicionar hosts, criar conexões do sistema de storage 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 plug-in do SnapCenter para VMware vSphere e Registrar o plug-in com o SnapCenter.

  Para obter mais informações, "Implante o plug-in do SnapCenter para VMware vSphere"consulte .

- Se os bancos de dados residirem em um sistema de arquivos VMDK, você deve ter feito login no vCenter e navegado para **opções de 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.

Passo 1: Impedir que o SnapCenter descubra entradas que não sejam do banco de dados

Você pode impedir que o SnapCenter descubra entradas não-banco de dados adicionadas no arquivo oratab.

Passos

1. Depois de instalar o plug-in para Oracle, o usuário root deve criar o arquivo **SC_oratab.config** sob o diretório */var/opt/SnapCenter/SCO/etc/*.

   Conceda a permissão de gravação ao proprietário e grupo binários Oracle para que o arquivo possa ser mantido no futuro.

2. O administrador do banco de dados deve adicionar as entradas não-banco de dados no arquivo **SC_oratab.config**.

   Recomenda-se manter o mesmo formato definido para as entradas não-banco de dados no arquivo */etc/oratab* ou o usuário pode simplesmente adicionar a string de entidade não-banco de dados.

   A cadeia é sensível a maiúsculas e minúsculas. Qualquer texto com número no início é Tratado como um comentário. O comentário pode ser anexado após o nome não-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-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.

Passo 2: Descubra recursos

Depois de instalar o plug-in, todos os bancos de dados nesse host são automaticamente descobertos e

exibidos na página recursos.

Os bancos de dados devem estar pelo menos no estado montado ou acima para que a descoberta dos bancos de dados seja bem-sucedida. Em um ambiente do Oracle Real Application clusters (RAC), a instância do banco de dados RAC no host onde a descoberta é executada deve estar pelo menos no estado montado ou acima para que a descoberta da instância do banco de dados seja bem-sucedida. Somente os bancos de dados que são descobertos com êxito podem ser adicionados aos grupos de recursos.

Se você tiver excluído um banco de dados Oracle no host, o servidor SnapCenter não estará ciente 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 **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** na lista **Exibir**.

   Clique em e selecione o nome do host e o tipo de banco de dados para filtrar os recursos. Em seguida, clique no ícone 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 está hospedado atualmente.

Resultados

Os bancos de dados são exibidos juntamente com informações como tipo de banco de dados, nome de host ou cluster, grupos e políticas de recursos 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 que não seja 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 storage que não é 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 protegida na coluna Estado 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 recursos. Você deve configurar credenciais de banco de dados para poder proteger o banco de dados ou adicioná-lo ao grupo de recursos para executar operações de proteção de dados.

Criar políticas de backup para bancos de dados Oracle

Antes de usar o SnapCenter para fazer backup dos recursos do banco de dados Oracle, você deve criar uma política de backup para o recurso ou para o grupo de recursos que deseja fazer backup. Uma política de backup é um conjunto de regras que regem como

você gerencia, agenda e retém backups. Você também pode especificar as configurações de replicação, script e tipo de backup. A criação de uma política economiza tempo quando você deseja reutilizar a política em outro recurso ou grupo de recursos.

Antes de começar

- Você precisa ter definido sua estratégia de backup.
- Você precisa se preparar para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, descobrir bancos de dados e criar conexões do sistema de storage.
- Se você estiver replicando snapshots em um storage secundário de espelhamento ou cofre, o administrador do SnapCenter deverá ter atribuído as SVMs a você para os volumes de origem e destino.
- Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios prescritor e postscript.
- Reveja os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror. Para obter informações, "Limites de objetos para sincronização ativa do SnapMirror" consulte .

Sobre esta tarefa

- SnapLock
  - Se a opção 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.

    Especificar um período de bloqueio instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na política.

    Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

> As configurações do SnapLock primário são gerenciadas na política de backup do SnapCenter e as configurações do SnapLock secundário são gerenciadas pelo ONTAP.

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 backup, execute as seguintes etapas:
   - Se pretender **criar uma cópia de segurança online**, selecione **cópia de segurança online**.

     Você deve especificar se deseja fazer backup de todos os arquivos de dados, arquivos de controle e arquivos de log de arquivamento, somente arquivos de dados e arquivos de controle ou somente arquivos de log de arquivamento.

- Se pretender **criar uma cópia de segurança offline**, selecione **cópia de segurança offline** e, em seguida, selecione uma das seguintes opções:
  - Se você quiser criar um backup off-line quando o banco de dados estiver no estado montado, selecione **montar**.
  - Se pretender criar uma cópia de segurança de encerramento offline alterando a base de dados para o estado de encerramento, selecione **Encerrar**.

    Se você estiver tendo bancos de dados conetáveis (PDBs) e quiser salvar o estado das PDBs antes de criar o backup, selecione **Salvar estado das PDBs**. Isso permite que você traga as PDBs ao seu estado original após a criação do backup.
- Especifique a frequência da programação selecionando **on demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.

  Você pode especificar a programação (data de início e data de término) para a operação de backup enquanto cria 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 diferentes programações de backup a cada política.

  Se você tiver agendado para as 2:00 da manhã, o horário não será acionado durante o horário de verão (DST).
- Se você quiser catalogar o backup usando o Oracle Recovery Manager (RMAN), selecione **Catálogo de backup com o Oracle Recovery Manager (RMAN)**.

  Você pode executar catalogação diferida para um backup de cada vez usando a GUI ou usando o comando SnapCenter CLI Catalog-SmBackupWithOracleRMAN.

  Se você quiser catalogar backups de um banco de dados RAC, verifique se nenhum outro trabalho está sendo executado para esse banco de dados. Se outro trabalho estiver em execução, a operação de catalogação falhará em vez de ficar na fila.
- Se você quiser podar logs de arquivo após o backup, selecione **Prune archive logs after backup**.

  A eliminação dos registos de arquivo do destino do registo de arquivo que não está configurado na base de dados será ignorada.

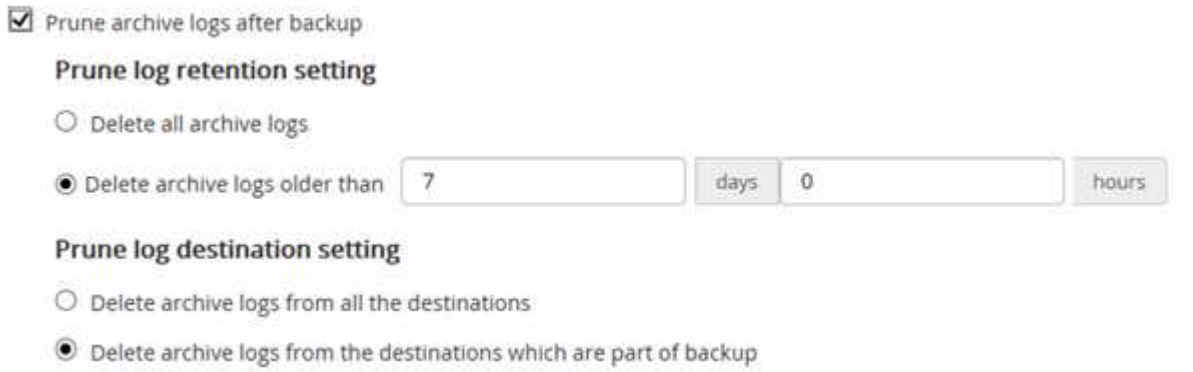
  Se você estiver usando o Oracle Standard Edition, você pode usar os parâmetros LOG_ARCHIVE_DEST e LOG_ARCHIVE_DUPLEX_DEST ao executar o backup do log de arquivamento.
- Só pode eliminar registos de arquivo se tiver selecionado os ficheiros de registo de arquivo como parte da cópia de segurança.

  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…
Eliminar todos os registos de arquivo	Selecione **Eliminar todos os registos de arquivo**.

Se você quiser…	Então…
Excluir Registros de arquivamento que são mais antigos	Selecione **Eliminar registos de arquivo mais antigos que** e, em seguida, especifique a idade dos registos de arquivo a eliminar em dias e horas.
Eliminar registos de arquivo de todos os destinos	Selecione **Eliminar registos de arquivo de todos os destinos**.
Elimine os registos de arquivo dos destinos de registo que fazem parte da cópia de segurança	Selecione **Eliminar registos de arquivo a partir dos destinos que fazem parte da cópia de segurança**.

+



7. Na página retenção, 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 instantâneos	Selecione **Total de cópias Snapshot a manter** e especifique o número de capturas instantâneas que deseja manter. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro. O valor máximo de retenção é 1018 para recursos no ONTAP 9.4 ou posterior e 254 para recursos no ONTAP 9.3 ou anterior. Os backups falharão se a retenção for definida para um valor maior do que o que a versão subjacente do ONTAP suporta. Você deve definir a contagem de retenção como 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino.
Mantenha as capturas instantâneas por um determinado número de dias	Selecione **manter cópias Snapshot para** e especifique o número de dias para os quais deseja manter as capturas instantâneas antes de excluí-las.
Período de bloqueio instantâneo	Selecione período de bloqueio de cópias instantâneas e selecione dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

Você pode reter backups de log de arquivamento somente se tiver selecionado os arquivos de log de arquivamento como parte do backup.

8. Na página replicação, especifique as configurações de replicação:

Para este campo…	Faça isso…
Atualize o SnapMirror depois de criar um instantâneo local	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Esta opção deve estar ativada para a 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.
Atualize o SnapVault depois de criar um instantâneo local	Selecione esta opção para executar a replicação de backup disco a disco (backups SnapVault). Quando o SnapLock é configurado apenas no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página topologia atualiza o período de bloqueio no secundário que é recuperado do ONTAP. Para obter mais informações sobre o SnapLock Vault, consulte "Armazene cópias Snapshot em WORM em um destino de cofre" "Veja os backups e clones do banco de dados Oracle na página topologia"Consulte .
Etiqueta de política secundária	Selecione uma etiqueta Snapshot. Dependendo do rótulo de captura instantânea selecionado, o ONTAP aplica a política de retenção de snapshot secundária que corresponde ao rótulo. Se você selecionou **Atualizar SnapMirror depois de criar uma cópia Snapshot local**, você pode especificar opcionalmente o rótulo de política secundária. No entanto, se você selecionou **Atualizar SnapVault depois de criar uma cópia Snapshot local**, especifique o rótulo de política secundária.

Para este campo…	Faça isso…
Contagem de tentativas de erro	Introduza o número máximo de tentativas de replicação que podem ser permitidas antes de a operação parar.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o storage secundário para evitar atingir o limite máximo de snapshots no storage secundário.

9. Na página Script, insira o caminho e os argumentos do prescritor ou postscript que você deseja executar antes ou depois da operação de backup, respetivamente.

   Você deve armazenar os prescripts e 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 qualquer pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

   Você também pode especificar o valor de tempo limite do script. O valor padrão é de 60 segundos.

   O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript. "Saiba 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 prescritor ou postscript que você deseja executar antes ou depois da operação de verificação, respetivamente.

       Você deve armazenar os prescripts e 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 qualquer pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

    Você também pode especificar o valor de tempo limite do script. O valor padrão é de 60 segundos.

11. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas para bancos de dados Oracle

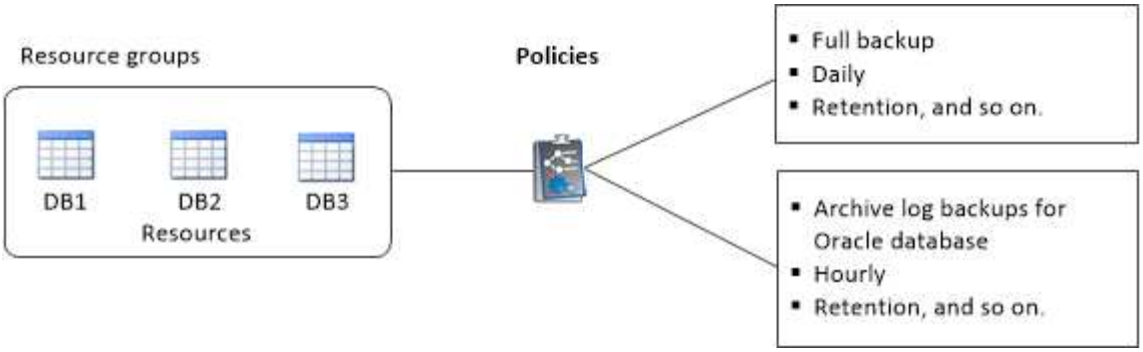
Um grupo de recursos é um contentor onde você adiciona recursos que deseja fazer backup e proteger. Um grupo de recursos permite fazer backup de todos os dados associados a um determinado aplicativo simultaneamente.

Sobre esta tarefa

- Um banco de dados com arquivos em grupos de discos ASM deve estar no estado "MOUNT" 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 tarefa de proteção de dados que deseja executar.

  A imagem a seguir ilustra a relação entre recursos, grupos de recursos e políticas para bancos de dados:



- Para políticas habilitadas para o SnapLock, para ONTAP 9.12,1 e versões abaixo, se você especificar um período de bloqueio do Snapshot, os clones criados a partir dos snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.
- A adição de novos bancos de dados sem a sincronização ativa do SnapMirror a um grupo de recursos existente que contenha recursos com a sincronização ativa do SnapMirror não é suportada.
- A adição de novos bancos de dados a um grupo de recursos existente no modo failover da sincronização ativa do SnapMirror não é suportada. Você pode adicionar recursos ao grupo de recursos apenas no estado regular ou de failback.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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. Introduza um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 carateres.

   b. Insira um ou mais rótulos no campo Tag para ajudá-lo a pesquisar o grupo de recursos mais tarde.

      Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.

   c. Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

      Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

   d. Especifique os destinos dos ficheiros de registo de arquivo que não pretende efetuar uma cópia de segurança.

      Você deve usar exatamente o mesmo destino que foi definido no Oracle, incluindo prefixo, se necessário.

4. Na página recursos, selecione um nome de host de banco de dados Oracle na lista suspensa **Host**.

   Os recursos são listados na seção recursos disponíveis somente se o recurso for descoberto com êxito. Se você tiver adicionado recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois de atualizar sua lista de recursos.

5. Selecione os recursos na 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 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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

   c. Na janela Adicionar programações para a política *policy_name*, configure a programação e clique em **OK**.

      Onde, *policy_name* é o nome da política selecionada.

      As programações configuradas são listadas na coluna agendas aplicadas.

   As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas de backup do SnapCenter.

7. Na página Verificação, execute as seguintes etapas:

   a. Clique em **carregar localizadores** para carregar os volumes SnapMirror ou SnapVault para executar a verificação no armazenamento secundário.

   b. Clique na coluna Configurar agendas 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…**
Execute a verificação após a cópia de segurança	Selecione **Executar verificação após backup**.
Marque uma verificação	Selecione **Executar verificação agendada** e, em seguida, selecione o tipo de agendamento na lista suspensa.

   d. Selecione **verificar no local secundário** para verificar os backups no sistema de armazenamento secundário.

   e. Clique em **OK**.

      As programações de verificação configuradas são listadas na coluna agendas aplicadas.

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 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-SmtpServer.

9. Revise o resumo e clique em **Finish**.

Faça backup dos recursos Oracle

Se um recurso não fizer parte de qualquer grupo de recursos, você poderá fazer backup do recurso na página recursos.

Passos

1. No painel de navegação esquerdo, selecione **Resources** e o plug-in apropriado na lista.
2. Na página recursos, selecione **Banco de dados** na lista Exibir.
3. Clique em e selecione o nome do host e o tipo de banco de dados para filtrar os recursos.

   Em seguida, pode clicar para fechar o painel de filtro.

4. Selecione o banco de dados que deseja fazer backup.

   A página Database-Protect (proteção de banco de dados) é exibida.

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 da captura Instantânea.

      Por exemplo, `customtext_policy_hostname` ou `resource_hostname`. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

   b. Especifique os destinos dos ficheiros de registo de arquivo que não pretende efetuar uma cópia de segurança.
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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique na coluna Configurar agendas para configurar uma agenda para a política desejada.
   c. Na janela Adicionar agendas para a política *policy_name* , configure a programação e `OK` selecione .

      policy_name é o nome da política selecionada.

As programações configuradas são listadas na coluna agendas aplicadas.

7. Na página Verificação, execute as seguintes etapas:
   a. Clique em **Load Locators** para carregar os volumes SnapMirror ou SnapVault para verificar o armazenamento secundário.
   b. Clique na coluna Configurar agendas para configurar o agendamento de verificação para todos os tipos de agendamento da política. Na caixa de diálogo Adicionar agendas 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, você não pode executar a operação de verificação em Leaf Nodes se a cardinalidade for menor que os nós numéricos no cluster RAC.

   e. Selecione **verificar no local secundário** para verificar os backups no armazenamento secundário.
   f. Clique em **OK**.

      As programações de verificação configuradas são listadas na coluna agendas aplicadas.

8. Na página notificação, selecione os cenários em que você deseja enviar os e-mails da 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 quiser anexar o relatório da operação de backup realizada no recurso, selecione **Anexar Relatório de trabalho**.

   Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando o comando GUI ou PowerShell `Set-SmSmtpServer` .

9. Revise o resumo e clique em **Finish**.

   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 tiver aplicado 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. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Depois de 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 residia.

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 do 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 `Set-SmConfigSettings` o cmdlet:

  Depois de 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 pode falhar com o código de erro DBV-00100 arquivo especificado. Você deve modificar os valores dos parâmetros VERIFICATION_DELAY e VERIFICATION_RETRY_COUNT em sco.properties.

  Depois de 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 ser capaz de detetar uma relação de proteção após um failover.
- Se você estiver fazendo backup de dados de aplicativos em VMDKs e o tamanho de heap Java para o plug-in SnapCenter para VMware vSphere não for grande o suficiente, o backup pode falhar.

  Para aumentar o tamanho do heap Java, localize o arquivo de script */opt/NetApp/init_scripts/scvservice*. Nesse script, o `do_start method` 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 detetar a relação SnapMirror ou SnapVault após o failover do MetroCluster"
- "O banco de dados Oracle RAC One Node é ignorado para a execução das operações do SnapCenter"
- "Falha ao alterar o estado de um banco de dados Oracle 12c ASM"
- "Parâmetros personalizáveis para operações de backup, restauração e clone em sistemas AIX" (Requer login)

Faça backup de grupos de recursos de banco de dados Oracle

Um grupo de recursos é uma coleção de recursos em um host ou cluster. A operação de backup é realizada 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 uma programação configurada, os backups serão criados de acordo com a programação.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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 em 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 um storage que não seja NetApp, a operação de backup será abortada mesmo que o outro banco de dados esteja no storage 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. Monitorize o progresso selecionando **Monitor > trabalhos**.

Depois de 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 residia.

  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 do 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 `Set-SmConfigSettings` o cmdlet:

  Depois de 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 pode falhar com o código de erro DBV-00100 arquivo especificado. Você deve modificar os valores dos parâmetros VERIFICATION_DELAY_ e VERIFICATION_RETRY_COUNT em sco.properties.

  Depois de 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 o backup do banco de dados Oracle

Saiba como monitorar o progresso das operações de backup e operações de proteção de dados.

Monitorar operações de backup de banco de dados Oracle

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado correspondente das

operações:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- 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 a que apenas as operações de cópia de segurança sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Backup**.
   d. Na lista suspensa **Status**, selecione o status da cópia de segurança.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.

   Embora o status do trabalho de backup seja exibido , quando você clica nos detalhes do trabalho, você pode ver que algumas das tarefas secundárias da operação de backup ainda estão em andamento ou marcadas com sinais de aviso.

5. Na página Detalhes da tarefa, clique em **Exibir logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Monitore operações de proteção de dados no painel atividade

O painel atividade exibe as cinco operações mais recentes executadas. O painel atividade também é exibido quando a operação foi iniciada e o status da operação.

O painel atividade exibe informações sobre operações de backup, restauração, clone e backup agendadas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 da tarefa**.

Outras operações de backup

Faça backup de bancos de dados Oracle usando comandos UNIX

O fluxo de trabalho de backup inclui Planejamento, identificação dos recursos para backup, criação de políticas de backup, criação de grupos de recursos e inclusão 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 servidor SnapCenter usando o comando *Open-SmConnection*.

  Você pode ter apenas uma sessão de login da conta do SnapCenter e o token é armazenado no diretório home do usuário.

  A sessão de ligação é válida apenas durante 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 servidor SnapCenter, descobrir as instâncias de banco de dados Oracle, adicionar política e grupo 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*. Em alternativa, pode também consultar o "Guia de Referência de comandos do software SnapCenter".

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado: *Open-SmConnection*
2. Execute a operação de descoberta de recursos do host: *Get-SmResources*
3. Configurar credenciais de banco de dados Oracle e nós preferenciais para operação de backup de um banco de dados do Real Application Cluster (RAC): *Configure-SmOracleDatabase*
4. Criar uma política de backup: *Add-SmPolicy*
5. Recuperar 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 secundária ao criar um grupo de recursos de backup.

6. Adicionar um grupo de recursos ao SnapCenter: *Adicionar-SmResourceGroup*
7. Criar um backup: *New-SmBackup*

   Você pode poll a tarefa usando a opção WaitForCompletion. Se essa opção for especificada, o comando

continuará a polling 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 as operações de backup em execução, na fila ou não responsivas.

Você deve estar conetado como administrador do SnapCenter ou proprietário da tarefa para cancelar as operações de backup.

Sobre esta tarefa

Quando você cancela uma operação de backup, o servidor SnapCenter interrompe a operação e remove todos os snapshots do armazenamento se o backup criado não estiver registrado no servidor SnapCenter. Se o backup já estiver registrado no servidor SnapCenter, ele não reverterá o instantâneo já criado mesmo após o cancelamento ser acionado.

- Pode cancelar apenas a operação de registo ou cópia de segurança completa que está em fila ou em execução.
- Não é possível cancelar a operação após a verificação ter sido iniciada.

  Se cancelar a operação antes da verificação, a operação é cancelada e a operação de verificação não será executada.

- Não é possível cancelar a operação de cópia de segurança depois de as operações de catálogo terem sido iniciadas.
- Pode cancelar uma operação de cópia de segurança a partir da página Monitor ou do painel atividade.
- Além de usar a GUI do SnapCenter, você pode usar comandos CLI para cancelar operações.
- O botão **Cancelar trabalho** está desativado 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 em fila de outros membros enquanto usa essa função.

Passo

Execute uma das seguintes ações:

A partir do…	Ação
Página do monitor	1. No painel de navegação esquerdo, clique em **Monitor** > **trabalhos**. 2. Selecione a operação e clique em **Cancelar trabalho**.

A partir do…	Ação
Painel da atividade	1. Depois de iniciar o trabalho de cópia de segurança, clique no painel atividade para ver as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

Resultados

A operação é cancelada e o recurso é revertido para o estado original.

Se a operação cancelada não for responsiva no estado de cancelamento ou execução, você deve executar o Cancelar-SmJob -JobID <int> -forçar para interromper a operação de backup com força.

Veja os backups e clones do banco de dados Oracle na página topologia

Ao se preparar para fazer backup ou clonar um recurso, talvez seja útil exibir uma representação gráfica de todos os backups e clones no storage primário e secundário.

Sobre esta tarefa

Na página topologia, você pode ver todos os backups e clones disponíveis para o grupo de recursos ou recursos selecionado. Você pode visualizar os detalhes desses backups e clones e, em seguida, selecioná-los para executar operações de proteção de dados.

Você pode revisar os ícones a seguir na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no storage primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups e clones disponíveis no storage primário.
- Exibe o número de backups e clones espelhados no storage secundário usando a tecnologia SnapMirror.
- Exibe o número de backups e clones replicados no storage secundário usando a tecnologia SnapVault.

  O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou backups 6 usando uma política para reter apenas 4 backups, o número de backups exibidos é 6.

Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

Se você tiver uma relação secundária como sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), você poderá ver os seguintes ícones adicionais:

- O site da réplica está em cima.
- O site da réplica está inativo.
- A relação do espelho secundário ou do cofre não foi restabelecida.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o recurso ou o 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 é exibida.

4. Revise o cartão de resumo para ver um resumo do número de backups e clones disponíveis no storage 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 **Refresh** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clique no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Um horário semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo é espalhado por vários volumes, o tempo de expiração do SnapLock para o backup será o tempo de expiração do SnapLock mais longo definido para um snapshot em um volume. O tempo de expiração mais longo do SnapLock é recuperado do ONTAP.

   Para a 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 a relação de sincronização ativa do SnapMirror.

   - Para a sincronização ativa do SnapMirror e somente para o ONTAP 9.14,1, as relações de espelhamento do Async ou EspelrorVault do Async com o novo destino primário devem ser configuradas manualmente após o failover. A partir do ONTAP 9.15,1 em diante, o espelho do Async ou o MirrorVault do Async 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 **Refresh** somente depois que um backup tiver sido criado.

5. No modo de 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 um 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, catálogo, descatálogo e exclusão.

Não é possível renomear ou excluir backups que estão no armazenamento secundário.

- Se tiver selecionado um backup de log, você só poderá executar operações de renomeação, montagem, desmontagem, catálogo, descatálogo e exclusão.
- Se você catalogou o backup usando o Oracle Recovery Manager (RMAN), não será possível renomear esses backups catalogados.

7. Se quiser excluir um clone, selecione-o na tabela e clique em .

Se o valor atribuído ao SnapmirrorStatusUpdateWaitTime for menor, as cópias de backup Mirror e Vault não serão listadas na página de topologia, mesmo que os volumes de dados e log sejam protegidos com êxito. Você deve aumentar o valor atribuído ao SnapmirrorStatusUpdateWaitTime usando o cmdlet *Set-SmConfigSettings* PowerShell.

As informações sobre os parâmetros que podem ser usados com o comando e suas descrições podem ser obtidas executando Get-Help *command_name*.

Em alternativa, pode também consultar a "Guia de Referência de comandos do software SnapCenter" ou "Guia de referência de cmdlet do software SnapCenter".

Montar e desmontar backups de bancos de dados

Você pode montar um único ou vários dados e Registrar somente backups se quiser acessar os arquivos no backup. Você pode montar o backup no mesmo host em que o backup foi criado ou em um host remoto com o mesmo tipo de configurações Oracle e host. Se você tiver montado manualmente os backups, deverá desmontar manualmente os backups após concluir a operação. Em qualquer instância, um backup de um banco de dados pode ser montado em qualquer um do host. 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 Leaf Nodes se a cardinalidade for menor que os nós numéricos 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 de Gerenciamento Automático de armazenamento (ASM) em um ambiente NFS e quiser montar os backups ASM, você deve ter adicionado o caminho de disco 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 ASM como parte de uma operação de recuperação, você deve ter adicionado o caminho de 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, "Como adicionar caminhos de disco ao ASM_diskstring"consulte .

- Você deve configurar as credenciais ASM e a porta ASM se for diferente da do host do banco de dados de origem durante a montagem do backup.
- Se você quiser montar em um host alternativo, verifique se o host alternativo atende aos seguintes requisitos:
  - O mesmo UID e GID do host original
  - Mesma versão Oracle que a do host original
  - A mesma distribuição e versão do sistema operacional que a do host original
  - Para NVMe, o NVMe útil deve ser instalado
- Você deve garantir que o LUN não seja mapeado para o host AIX usando o iGroup que consiste em protocolos mistos iSCSI e FC. Para obter mais informações, "A operação falha com erro não é possível descobrir o dispositivo para LUN"consulte .

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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** no sistema de armazenamento primário ou secundário (espelhado ou replicado).
5. Selecione o backup na tabela e clique em .
6. Na página Monte 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 de terminar

- Você pode executar o seguinte comando para recuperar as informações relacionadas ao backup montado:

  ```
  ./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
  ```

- Se tiver montado uma base de dados ASM, pode executar o seguinte comando para recuperar as informações relacionadas com a cópia de segurança montada:

  ```
  ./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*. Em alternativa, pode também 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 arquivos no backup.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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.

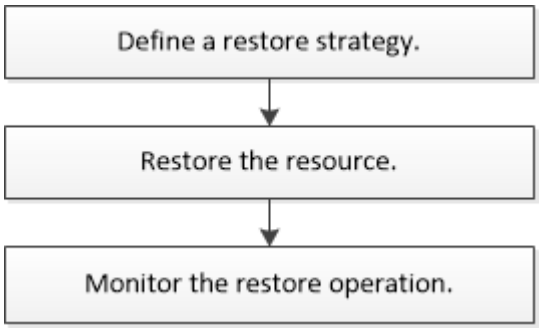
4. Selecione a cópia de segurança montada e, em seguida, clique em .
5. Clique em **OK**.

Restaurar e recuperar bancos de dados Oracle

Restaure o fluxo de trabalho

O fluxo de trabalho de restauração inclui Planejamento, execução das 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 você possa executar operações de restauração e recuperação com sucesso.

Tipos de backups suportados para operações de restauração e recuperação

O SnapCenter dá suporte à restauração e recuperação de diferentes tipos de backups de bancos de dados Oracle.

- Backup de dados on-line
- Backup de dados de desligamento off-line
- Backup de dados de montagem off-line

> Se você estiver restaurando um desligamento off-line ou backup de dados de montagem off-line, o SnapCenter deixa o banco de dados no estado off-line. Você deve recuperar manualmente o banco de dados e redefinir os logs.

- Backup completo
- Backups de montagem off-line de bancos de dados em espera do Data Guard
- Backups on-line somente de dados de bancos de dados em espera do ative Data Guard

> Não é possível executar a recuperação de bancos de dados em espera do ative 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 RAC (Real Application clusters)
- Backups de dados on-line, backups completos online, backups de montagem off-line e backups de desligamento off-line em uma configuração de gerenciamento de armazenamento automático (ASM)

Tipos de métodos de restauração suportados para bancos de dados Oracle

O SnapCenter é compatível com 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 que o sistema de arquivos seja usado para restauração sem perda de dados.

> O SnapCenter não é compatível com 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 de conexão e cópia 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 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 do Flex ASM (em que a cardinalidade é menor do que os nós numéricos no cluster RAC) ou bancos de dados do ASM RAC no VMDK ou RDM, somente o método de restauração de conexão e cópia é suportado.

Mesmo que você tenha ativado com força a restauração no local, o SnapCenter executa a restauração de conexão e cópia nos seguintes cenários:

- Faça a restauração a partir do sistema de storage secundário e, se o Data ONTAP for anterior a 8,3
- Restauração de grupos de discos ASM presentes em nós de uma configuração do Oracle RAC em que a instância de banco de dados não está configurada
- Na configuração do Oracle RAC, em qualquer um dos nós pares se a instância ASM ou a instância de cluster não estiver em execução ou se o nó peer estiver inativo
- Restauração de arquivos de controle somente
- Restaure um subconjunto de espaços de tablespaces que residem em um grupo de discos ASM
- O grupo de discos é partilhado entre ficheiros de dados, ficheiro SP e ficheiro de palavra-passe
- 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 servidor SnapCenter 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 na pilha de armazenamento e banco de dados, a restauração no local é realizada, em que a restauração do arquivo ou LUN é realizada no ONTAP. O SnapCenter suporta apenas o SFSR (Single File SnapRestore) como parte do método de restauração no local.

O Data ONTAP 8.3 ou posterior oferece suporte à restauração no local a partir de um local secundário.

Se você quiser executar a restauração no local no banco de dados, verifique se você tem somente datafiles no grupo de discos ASM. Você deve criar um backup depois que quaisquer alterações forem feitas no grupo de discos ASM ou na estrutura física do banco de dados. Depois de 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 o ponto de montagem corresponder aos seguintes critérios:

- Não são adicionados dados novos após a cópia de segurança (verificação de ficheiro estrangeiro)
- Sem adição, exclusão ou recriação de disco ASM ou LUN após backup (verificação de alteração estrutural do grupo de discos ASM)
- Sem adição, exclusão ou recriação de LUNs ao grupo de discos LVM (verificação de alteração estrutural do grupo de discos LVM)

Você também pode habilitar a restauração no local com força usando GUI, CLI do SnapCenter ou cmdlet do PowerShell para substituir a verificação de arquivo estrangeiro e a verificação de alteração estrutural do grupo de discos LVM.

Executar a restauração no local no ASM RAC

No SnapCenter, o nó no qual você executa a restauração é denominado como nó principal e todos os outros nós do RAC no qual reside o grupo de discos ASM são chamados de nós de ponto. O SnapCenter altera o estado do grupo de discos ASM para desmontar em todos os nós em que o grupo de discos ASM está no estado de montagem antes de executar a operação de restauração de storage. Após a conclusão da restauração de armazenamento, o SnapCenter altera o estado do grupo de discos ASM como era antes da operação de restauração.

Em ambientes SAN, o SnapCenter remove dispositivos de todos os nós de mesmo nível e executa a operação de desmapear LUN antes da operação de restauração de storage. Após a operação de restauração de storage, o SnapCenter executa operações de mapa LUN e constrói dispositivos em todos os nós de mesmo nível. Em um ambiente SAN, se o layout ASM do Oracle RAC estiver residindo em LUNs, em seguida, durante a restauração do SnapCenter, executa operações de desmapeamento de LUN, restauração de LUN e mapa de LUN em todos os nós do cluster RAC onde reside o grupo de discos ASM. Antes de restaurar, mesmo que todos os iniciadores dos nós RAC não fossem usados para os LUNs, depois de restaurar 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 de pares, o SnapCenter reverte automaticamente o estado do grupo de discos ASM como era antes de executar a restauração em nós de pares nos quais a operação de pré-restauração foi bem-sucedida. A reversão não é suportada para o nó principal e o nó ponto em que a operação falhou. Antes de tentar outra restauração, você deve corrigir manualmente o problema no nó peer 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 nenhum retorno será executado. Antes de tentar outra restauração, você deve corrigir manualmente o problema de restauração de armazenamento e colocar o grupo de discos ASM no nó principal de volta ao estado de montagem.
- Se houver alguma falha durante a atividade do Postrestore em qualquer um dos nós pares, o SnapCenter continuará com a operação de restauração nos outros nós de mesmo nível. Você deve corrigir manualmente o problema de pós-restauração no nó peer.

Tipos de operações de restauração compatíveis com bancos de dados Oracle

O SnapCenter permite executar 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 arquivos ausentes quando comparados aos arquivos de banco de dados reais.

Restauração completa

- Restaura apenas os arquivos de dados
- Restaura apenas os arquivos de controle
- Restaura os arquivos de dados e controle
- Restaura arquivos de dados, controla arquivos e refaz arquivos de log em bancos de dados de espera do Data Guard e ative Data Guard

Restauração parcial

- Restaura apenas os espaços de tabela selecionados
- Restaura apenas os bancos de dados conetáveis selecionados (PDBs)
- Restaura apenas os espaços de tabela selecionados de um PDB

Tipos de operações de recuperação compatíveis com bancos de dados Oracle

O SnapCenter permite executar 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 específico de mudança de sistema (SCN)

- A base de dados até uma data e hora específicas

  Você deve especificar a data e a hora para recuperação com base no fuso horário do host do banco de dados.

  O SnapCenter também fornece a opção sem recuperação para bancos de dados Oracle.

> O plug-in para banco de dados Oracle não suporta 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 precisa 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 estará no estado suspenso quando você executar o comando *renamedg*. Você pode aplicar o Oracle patch 19544733 para corrigir esse problema.

As seguintes operações de restauração e recuperação não são suportadas:

- Restauração e recuperação de espaços de tablespaces do banco de dados de contentor raiz (CDB)
- Restauração de espaços de tablespaces temporários e espaços de tablespaces temporários associados a PDBs
- Restauração e recuperação de espaços de tablespaces de vários PDBs simultaneamente
- Restauração de backups de log
- Restauração de backups para um local diferente
- Restauração de arquivos de log refazer em qualquer configuração que não seja os bancos de dados de espera do Data Guard ou do ative Data Guard
- Restauração do arquivo SPFILE e Senha
- Quando você executa uma operação de restauração em um banco de dados que foi recriado usando o nome do banco de dados pré-existente no mesmo host, foi gerenciado pelo SnapCenter e teve 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 qualquer uma das seguintes ações:

  - Descubra os recursos do SnapCenter depois que o banco de dados for recriado
  - Crie uma cópia de segurança da base de dados recriada

Limitações relacionadas à recuperação ponto-em-tempo de tablespaces

- A recuperação pontual (PITR) do SISTEMA, SYSAUX e DESFAZER espaços DE tablespaces não é suportada
- PITR de tablespaces não pode ser executado junto com outros tipos de restauração
- Se um espaço de tabela for renomeado e você quiser recuperá-lo para um ponto antes de ser renomeado, você deve especificar o nome anterior do espaço de tabela
- Se as restrições para as tabelas em um espaço de tabela estiverem contidas em outro espaço de tabela, você deve recuperar ambas as espaço de tabela

- Se uma tabela e seus índices forem armazenados em diferentes espaços de tabela, então os índices devem ser descartados antes de executar o PITR
- O PITR não pode ser usado para recuperar o espaço de tabela padrão atual
- O PITR não pode ser usado para recuperar tablespaces contendo qualquer um dos seguintes objetos:
  - Objetos com objetos subjacentes (como vistas 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 forem armazenadas em diferentes espaços de tabela, então você deve soltar a tabela antes de executar o PITR ou mover todas as partições para a mesma espaço de tabela antes de executar o PITR.

  - Desfazer ou reverter segmentos
  - Filas avançadas compatíveis com Oracle 8i 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, Privileges, dimensões, diretórios e sequências.

Fontes e destinos para restaurar bancos de dados Oracle

É possível restaurar um banco de dados Oracle a partir de uma cópia de backup no storage primário ou no storage secundário. Você só pode restaurar bancos de dados para o mesmo local na mesma instância de banco de dados. No entanto, na configuração do Real Application Cluster (RAC), você pode restaurar bancos de dados para outros nós.

Fontes para operações de restauração

É possível restaurar bancos de dados a partir de um backup no storage primário ou no storage secundário. Se você quiser restaurar a partir de um backup no storage secundário em uma configuração de vários espelhos, você pode selecionar o espelho de armazenamento secundário como a origem.

Destinos para operações de restauração

Você só pode restaurar bancos de dados para o 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 prescrição específica e postscript

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript enquanto restaura uma base de dados.

Variáveis de ambiente predefinidas suportadas para restaurar um banco de dados

- **SC_JOB_ID** especifica a ID da tarefa 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 banco de dados separados por pipe.

Exemplo: NFSB31

- **SC_HOST** especifica o nome do host do banco de dados.

  Esse 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: oracle

- **SC_os_GROUP** especifica o grupo do sistema operacional do banco de dados.

  Exemplo: Oinstall

- **SC_BACKUP_NAME** especifica o nome do backup.

  Esse 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_22_12.16.48.9267-1-2021_07_21,RG2_scspr2417819002_07-scspr2417819002-2021_12.16.48.9267_1

- **SC_BACKUP_ID** especifica o ID do backup.

  Esse 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 at 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 são recuperados e também o escopo de recuperação.

  Exemplo: RESTORESCOPE:usingBackupControlfile:false|RECOVERYSCOPE:allLogs

Para obter informações sobre delimitadores, "Delimitadores suportados"consulte .

Requisitos para restaurar um banco de dados Oracle

Antes de restaurar um banco de dados Oracle, você deve garantir que os pré-requisitos sejam concluídos.

- Você deve ter definido sua estratégia de restauração e recuperação.
- O administrador do SnapCenter deve ter atribuído as máquinas virtuais de storage (SVMs) para os volumes de origem e de destino se você estiver replicando snapshots em um espelho ou cofre.
- Se os logs de arquivo forem podados como parte do backup, você deve ter montado manualmente os backups de log de arquivamento necessários.
- Se você quiser restaurar bancos de dados Oracle que residem em um VMDK (Virtual Machine Disk), você deve garantir 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 sejam protegidos se a proteção secundária estiver ativada para esse banco de dados.
- Você deve garantir que o banco de dados RAC One Node esteja no estado "nomount" para executar o arquivo de controle ou restauração completa do banco de dados.
- Se você tiver uma instância de banco de dados ASM no ambiente NFS, adicione o caminho de disco ASM */var/opt/SnapCenter/scu/clones/*/** ao caminho existente definido no parâmetro ASM_diskstring para montar com êxito os backups de log 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 listener 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 tiver desabilitado a autenticação do SO e habilitado a autenticação de banco de dados Oracle para um banco de dados Oracle, e desejar restaurar os arquivos de dados e 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, é apresentada uma mensagem de aviso. Se ignorar o aviso e continuar, a restauração a partir do RDM falhará.

- Você deve garantir que o LUN não seja mapeado para o host AIX usando o iGroup que consiste em protocolos mistos iSCSI e FC. Para obter mais informações, "A operação falha com erro não é possível descobrir o dispositivo para LUN"consulte .

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 o seu sistema de arquivos ativo e, em seguida, recuperar o banco de dados.

Antes de começar

Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios prescritor e postscript.

Sobre esta tarefa

- A recuperação é efetuada utilizando os registos de arquivo disponíveis no local de registo de arquivo 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 refazer em um ou mais destinos off-line, conhecidos coletivamente como o log refazer arquivado. O SnapCenter identifica e monta o número ideal de backups de log com base na opção SCN especificada, data e hora selecionadas ou todos os logs. Se os logs de arquivo necessários para recuperação não estiverem disponíveis no local configurado, você deverá montar o instantâneo contendo os logs e especificar o caminho como logs de arquivo externo.

  Se você migrar o banco de dados ASM do ASMLIB para o ASMFD, os backups criados com o ASMLIB não podem ser usados para restaurar o banco de dados. Você deve criar backups na configuração ASMFD e usar esses backups para restaurar. Da mesma forma, se o banco de dados ASM for migrado do ASMFD para o ASMLIB, você deverá criar backups na configuração ASMLIB para restaurar.

  Quando você restaura um banco de dados, um arquivo de bloqueio operacional (.SM_lock_dbsid) é criado no host de banco de dados Oracle no diretório */var/opt/SnapCenter/SCO/lock* para evitar que várias operações sejam executadas no banco de dados. Depois que o banco de dados foi restaurado, o arquivo de bloqueio operacional é removido automaticamente.

  A restauração do arquivo SPFILE e Senha não é suportada.

- Para políticas habilitadas para o SnapLock, para ONTAP 9.12,1 e versões abaixo, se você especificar um período de bloqueio do Snapshot, os clones criados a partir dos snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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** nos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
5. Selecione a cópia de segurança na tabela e, em seguida, clique em * .
6. Na página Restaurar escopo, execute as seguintes tarefas:

   a. Se você tiver selecionado um backup de um banco de dados em um ambiente de Real Application clusters (RAC), selecione o nó RAC.

   b. Quando você seleciona um dado espelhado ou de cofre:

      - se não houver backup de log no mirror ou vault, nada será selecionado e os localizadores estarão vazios.
      - se existirem cópias de segurança de registo no mirror ou no vault, a cópia de segurança de registo

mais recente é selecionada e o localizador correspondente é apresentado.

> Se a cópia de segurança de registo selecionada existir na localização do espelho e do cofre, ambos os localizadores são apresentados.

c. Execute as seguintes ações:

Se você quiser restaurar…	Faça isso…
Todos os arquivos de dados do banco de dados	Selecione **todos os dados**. Somente os arquivos de dados do banco de dados são restaurados. Os ficheiros de controlo, os registos de arquivo ou os ficheiros de registo de refazer não são restaurados.
Tablespaces	Selecione **tablespaces**. Você pode especificar os espaços de tablespaces que você deseja restaurar.
Controlar ficheiros	Selecione **Control Files**. Durante a restauração de arquivos de controle, certifique-se de que a estrutura de diretórios existe ou deve ser criada com os proprietários corretos 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, o trabalho de restauro falhará.
Refazer ficheiros de registo	Selecione **Refazer arquivos de log**. Esta opção está disponível apenas para bancos de dados em espera do Data Guard ou em espera do ative Data Guard. Os ficheiros de registo de refazer não são salvaguardados para bases 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 arquivo.
Bancos de dados conetáveis (PDBs)	Selecione **bancos de dados conetáveis** e especifique as PDBs que você deseja restaurar.

Se você quiser restaurar…	Faça isso…
Espaço de tabela de banco de dados conetável (PDB)	Selecione * espaços de tabela de base de dados Pluggable (PDB)* e especifique o PDB e os espaços de tabela desse PDB que você deseja restaurar. Esta opção só está disponível se tiver selecionado um PDB para restauro.

d. Selecione **altere o estado do banco de dados, se necessário, para restaurar e recuperar** 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 de cima para baixo são abertos, montados, iniciados e desligados. Você deve selecionar essa caixa de seleção se o banco de dados estiver em um estado mais alto, 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 tiver de 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 restaurar, o banco de dados precisar estar no estado montado, o estado do banco de dados será alterado somente se você selecionar essa caixa de seleção.

a. Selecione **forçar restauração no local** se você quiser executar a restauração no local nos cenários em que novos arquivos de dados são adicionados após o backup ou quando LUNs são adicionados, excluídos ou recriados a um grupo de discos LVM.

7. Na página Recovery Scope (Escopo de recuperação), execute as seguintes ações:

Se você…	Faça isso…
Deseja recuperar para a última transação	Selecione **todos os registos**.
Deseja recuperar para um número específico de mudança de sistema (SCN)	Selecione **até SCN (número de mudança do sistema)**.
Deseja recuperar dados e tempo específicos	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**.

Se você…	Faça isso…
Deseja especificar quaisquer locais de registo de arquivo externo	Se o banco de dados estiver sendo executado no modo ARCHIVELOG, o SnapCenter identifica e monta o número ideal de backups de log com base na opção SCN especificada, data e hora selecionadas ou todos os logs. Se você ainda quiser especificar a localização dos arquivos de log de arquivo externo, selecione **especificar locais de log de arquivo externo**. Se os logs de arquivo forem podados como parte do backup e você tiver montado manualmente os backups de log de arquivamento necessários, você deve especificar o caminho de backup montado como o local de 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 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 só pode restaurar selecionando **sem recuperação**.

Se você estiver recuperando um banco de dados RAC com a opção abrir banco de dados selecionada, somente a instância RAC em que a operação de recuperação foi iniciada será devolvida ao estado aberto.

A recuperação não é suportada para bancos de dados de espera do Data Guard e ative Data Guard.

8. Na página PreOps, insira o caminho e os argumentos do prescritor que deseja executar antes da operação de restauração.

   Você deve armazenar as prescrições no caminho */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 qualquer pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

   Você também pode especificar o valor de tempo limite do script. O valor padrão é de 60 segundos.

   O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript. "Saiba 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 qualquer 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.

   Depois de restaurar um banco de dados de contentor (CDB) com ou sem arquivos de controle, ou depois de restaurar apenas arquivos de controle CDB, se você especificar para abrir o banco de dados após a recuperação, apenas o CDB será aberto e não os bancos de dados conetáveis (PDB) nesse CDB.

   Em uma configuração RAC, somente a instância RAC usada para recuperação é aberta após a recuperação.

   ⓘ Depois de restaurar um espaço de tabela do usuário com arquivos de controle, uma espaço de tabela do sistema com ou sem arquivos de controle, ou um PDB com ou sem arquivos de controle, apenas o estado do PDB relacionado à operação de restauração é alterado para o estado original. O estado das outras PDBs que não foram usadas para restauração não é alterado para o estado original porque o estado dessas PDBs não foi salvo. Você deve alterar manualmente o estado das PDBs que não foram usadas para restauração.

10. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários em que 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 pretender anexar o relatório da operação de restauro efetuada, tem de selecionar **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-SmtpServer.

11. Revise o resumo e clique em **Finish**.
12. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Para mais informações

- "O banco de dados Oracle RAC One Node é ignorado para a execução das operações do SnapCenter"
- "Falha ao restaurar a partir de um local secundário de SnapMirror ou SnapVault"
- "Falha ao restaurar a partir de um backup de uma encarnação órfã"
- "Parâmetros personalizáveis para operações de backup, restauração e clone em sistemas AIX"

Restaure e recupere espaços de tablespaces usando recuperação ponto no tempo

Você pode restaurar um subconjunto de espaços de tablespaces que foi corrompido ou

descartado sem afetar os outros espaços de tablespaces no banco de dados. O SnapCenter usa o RMAN para executar a recuperação pontual (PITR) dos espaços das tabelas.

Antes de começar

- Os backups que são necessários para executar PITR de tablespaces devem ser catalogados e montados.
- Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios prescritor 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 pode reutilizar um dos locais montados em vez de um ponto de montagem dedicado.

Você deve especificar a data e hora ou SCN e o espaço de tabela é restaurado no banco de dados de origem.

Você pode selecionar e restaurar vários espaços de tabela que residem em ambientes ASM, NFS e SAN. Por exemplo, se as tablespaces TS2 e TS3 residem em NFS e TS4 residem em SAN, você pode executar em uma única operação PITR para restaurar todos os espaços de tabela.

Em uma configuração RAC, você pode executar PITR de espaços de tablespaces de qualquer nó do RAC.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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) 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** nos sistemas de armazenamento primário ou secundário (espelhado ou replicado).

   Se o backup não estiver catalogado, selecione o backup e clique em **Catálogo**.

5. Selecione a cópia de segurança catalogada e, em seguida, clique em * .
6. Na página Restaurar escopo, execute as seguintes tarefas:
   a. Se você tiver selecionado um backup de um banco de dados em um ambiente de Real Application clusters (RAC), selecione o nó RAC.
   b. Selecione **tablespaces** e especifique as tablespaces que você deseja restaurar.

      Você não pode executar PITR em SYSAUX, SISTEMA e DESFAZER espaços de tablespaces.

   c. Selecione **altere o estado do banco de dados, se necessário, para restaurar e recuperar** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração

e recuperação.

7. Na página Recovery Scope (Escopo de recuperação), execute uma das seguintes ações:
   - Se você quiser recuperar para um número específico de mudança de sistema (SCN), selecione **até SCN** e especifique o SCN e o destino auxiliar.
   - Se pretender recuperar para uma data e hora específicas, selecione **Data e hora** e especifique a data e hora e o destino auxiliar.

     O SnapCenter identifica e monta e cataloga o número ideal de backups de dados e log 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 do prescritor que deseja executar antes da operação de restauração.

   Você deve armazenar as prescripts no caminho /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 qualquer pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

   Você também pode especificar o valor de tempo limite do script. O valor padrão é de 60 segundos.

   O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript. "Saiba 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 em que deseja enviar as notificações por e-mail.
11. Revise o resumo e clique em **Finish**.
12. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Restaurar e recuperar banco de dados conetável usando recuperação pontual

Você pode restaurar e recuperar um banco de dados conetável (PDB) que foi corrompido ou descartado sem afetar as outras PDBs no banco de dados de contentores (CDB). O SnapCenter usa o RMAN para executar a recuperação pontual (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 (mudando o estado para MONTADO) em todos os nós da configuração RAC.

- Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de

execução aos diretórios prescritor 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 pode 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 ESCRITA, LEITURA SOMENTE ou descartados, incluindo datafiles.

Você pode restaurar e recuperar apenas:

- Um PDB de cada vez
- Um espaço de tabela em um PDB
- Várias tablespaces do mesmo PDB

Em uma configuração RAC, você pode executar PITR de espaços de tablespaces de qualquer nó do RAC.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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) 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** nos sistemas de armazenamento primário ou secundário (espelhado ou replicado).

   Se o backup não estiver catalogado, selecione o backup e clique em **Catálogo**.

5. Selecione a cópia de segurança catalogada e, em seguida, clique em * .
6. Na página Restaurar escopo, execute as seguintes tarefas:
   a. Se você tiver selecionado um backup de um banco de dados em um ambiente de Real Application clusters (RAC), selecione o nó RAC.
   b. Dependendo se você deseja restaurar o PDB ou espaços de tabela em um PDB, execute uma das ações:

Se você quiser…	Passos…

Restaure um PDB	i. Selecione **bancos de dados conetáveis (PDBs)**. ii. Especifique o PDB que deseja restaurar. Você não pode executar PITR no banco de dados PDB.
Restaure espaços de tabela em um PDB	i. Selecione **espaços de tabela de base de dados conetáveis (PDB)**. ii. Especifique o PDB. iii. Especifique um único espaço de tabela ou vários espaços de tabela que você deseja restaurar. Você não pode executar PITR em SYSAUX, SISTEMA e DESFAZER espaços de tablespaces.

c. Selecione **altere o estado do banco de dados, se necessário, para restaurar e recuperar** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.

7. Na página Recovery Scope (Escopo de recuperação), execute uma das seguintes ações:
   - Se você quiser recuperar para um número específico de mudança de sistema (SCN), selecione **até SCN** e especifique o SCN e o destino auxiliar.
   - Se pretender recuperar para uma data e hora específicas, selecione **Data e hora** e especifique a data e hora e o destino auxiliar.

     O SnapCenter identifica e monta e cataloga o número ideal de backups de dados e log 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 do prescritor que deseja executar antes da operação de restauração.

   Você deve armazenar as prescripts no caminho /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 qualquer pasta dentro desse caminho para armazenar os scripts, você deve especificar essas pastas no caminho.

   Você também pode especificar o valor de tempo limite do script. O valor padrão é de 60 segundos.

   O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript. "Saiba 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 apenas no nó em que o banco de dados foi recuperado. Você deve abrir manualmente o PDB recuperado em todos os outros nós da configuração RAC.

10. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários em que deseja enviar as notificações por e-mail.
11. Revise o resumo e clique em **Finish**.
12. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Restaure e recupere bancos de dados Oracle usando comandos UNIX

O fluxo de trabalho de restauração e recuperação inclui o Planejamento, a execução das operações de restauração e recuperação e o monitoramento das operações.

Sobre esta tarefa

- Você deve executar os seguintes comandos para estabelecer a conexão com o servidor SnapCenter, listar os backups e 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*. Em alternativa, pode também 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 no local principal.

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 as informações detalhadas sobre o backup de um recurso especificado com um determinado ID de backup. As informações incluem nome do banco de dados, versão, home, start e end SCN, tablespaces, bancos de dados conetáveis e suas tablespaces.

4. Restaure dados do backup: *Restore-SmBackup*

Monitorar operações de restauração de banco de dados Oracle

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um 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 executar.

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Restore**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Cancelar operações de restauração de banco de dados Oracle

Você pode cancelar trabalhos de restauração que estão na fila.

Você deve estar logado como administrador do SnapCenter ou proprietário da tarefa para cancelar as operações de restauração.

Sobre esta tarefa

- Você pode cancelar uma operação de restauração em fila na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de restauração em execução.
- Você pode usar a GUI do SnapCenter, cmdlets do PowerShell ou os comandos CLI para cancelar as operações de restauração em fila.
- O botão **Cancelar trabalho** está desativado para operações de restauração que não podem ser canceladas.
- Se você selecionou **todos os membros desta função podem ver e operar em outros objetos membros** na página usuários/grupos ao criar uma função, você pode cancelar as operações de restauração em fila de outros membros enquanto usa essa função.

Passo

Execute uma das seguintes ações:

A partir 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 da atividade	1. Depois de iniciar a operação de restauração, clique no painel atividade para exibir as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

Clonar banco de dados Oracle

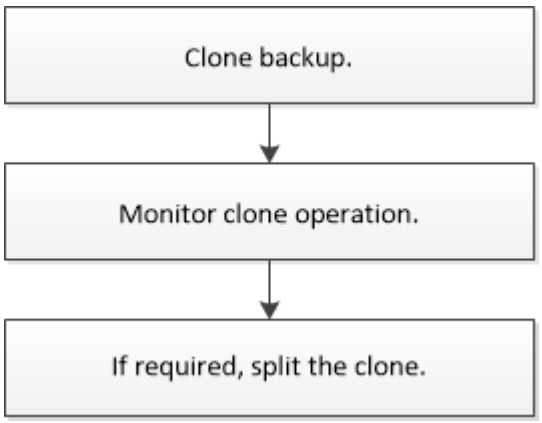
Fluxo de trabalho clone

O fluxo de trabalho do clone inclui Planejamento, execução da operação do clone e monitoramento da operação.

Você pode clonar bancos de dados pelos seguintes motivos:

- Para testar a funcionalidade que deve ser implementada usando a estrutura e o conteúdo atuais do banco de dados durante os ciclos de desenvolvimento de aplicativos.
- Para preencher depósitos de dados 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 clone:



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 compatíveis para clonagem

O SnapCenter é compatível com a clonagem de diferentes tipos de backup de bancos de dados Oracle.

- Backup de dados on-line
- Backup completo online
- Backup de montagem off-line
- Backup de desligamento off-line
- Backups de bancos de dados em espera do Data Guard e bancos de dados em espera do ative 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 RAC (Real Application clusters)
- Backups de dados on-line, backups completos online, backups de montagem off-line e backups de desligamento off-line em uma configuração de gerenciamento de armazenamento automático (ASM)

> As configurações SAN não são suportadas se a opção user_friendly_names no arquivo de configuração multipath estiver definida como yes.

> A clonagem de backups de log de arquivamento não é suportada.

Tipos de clonagem compatíveis com bancos de dados Oracle

Em um ambiente de banco de dados Oracle, o SnapCenter é compatível com a clonagem de um backup de banco de dados. Você pode clonar o backup de sistemas de storage primário e secundário.

O servidor SnapCenter usa a tecnologia NetApp FlexClone para clonar backups.

Você pode atualizar um clone executando o comando "Refresh-SmClone". Esse comando cria um backup do banco de dados, exclui o clone existente e cria um clone com o mesmo nome.

> A operação de atualização de clone só pode ser executada usando os comandos UNIX.

Convenções de nomenclatura de clones para bancos de dados Oracle

No SnapCenter 3,0, a convenção de nomenclatura usada para clones de sistemas de arquivos é diferente dos clones dos 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 clone 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 clone estará no estado suspenso quando você executar o comando *renamedg*. Você pode aplicar o Oracle patch 19544733 para corrigir esse problema.
- A clonagem de bancos de dados de um LUN que está diretamente conetado 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 outro host Windows, ou vice-versa, não é suportada.
- O diretório raiz do ponto de montagem do volume não pode ser um diretório partilhado.
- Se você mover um LUN que contém um clone para um novo volume, o clone não poderá ser excluído.

Variáveis de ambiente predefinidas para o prescritor específico de clone e postscript

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript durante a clonagem de uma base de dados.

Variáveis de ambiente predefinidas suportadas para clonar um banco de dados

- **SC_ORIGINAL_SID** especifica o SID do banco de dados de origem.

  Esse parâmetro será preenchido para volumes de aplicativos.

  Exemplo: NFSB32

- **SC_ORIGINAL_HOST** especifica o nome do host de origem.

  Esse 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.

  Esse 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_07_22-20-1_12.16.48.9267_12.16.48.9267,RG2_2021_07-21-scspr2417819002_1_2021,RG2_scspr2417819002_scspr2417819002-07-2021_12.16.48.9267_1

- **SC_AV_NAME** especifica os nomes dos volumes da aplicação.

  Exemplo: AV1|AV2

- **SC_ORIGINAL_os_USER** especifica o proprietário do sistema operacional do banco de dados de origem.

  Exemplo: oracle

- **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 do clone PDB, o valor deste parâmetro não será predefinido.

  Esse parâmetro será preenchido para volumes de aplicativos.

  Exemplo: Clonedb

- **SC_TARGET_HOST** especifica o nome do host onde o banco de dados será clonado.

  Esse 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 do clone PDB, o valor deste parâmetro não será predefinido.

  Exemplo: oracle

- **SC_TARGET_os_GROUP** especifica o grupo do sistema operacional do banco de dados clonado.

  Para o fluxo de trabalho do clone PDB, o valor deste parâmetro não será predefinido.

  Exemplo: Oinstall

- **SC_TARGET_DB_port** especifica a porta de banco de dados do banco de dados clonado.

  Para o fluxo de trabalho do clone PDB, o valor deste parâmetro não será predefinido.

  Exemplo: 1521

Para obter informações sobre delimitadores, "Delimitadores suportados"consulte .

Requisitos para clonar um banco de dados Oracle

Antes de clonar um banco de dados Oracle, você deve garantir que os pré-requisitos sejam concluídos.

- Você deve ter criado um backup do banco de dados usando o SnapCenter.

  Você deve ter criado com êxito os backups de dados on-line e de log ou backups off-line (montagem ou desligamento) para que a operação de clonagem seja bem-sucedida.

- Se você quiser personalizar o arquivo de controle ou refazer caminhos de arquivo de log, você deve ter pré-provisionado o sistema de arquivos necessário ou o grupo de discos de Gerenciamento Automático de armazenamento (ASM).

Por padrão, os arquivos de log refazer e 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 você estiver usando ASM em 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, "Como adicionar caminhos de disco ao ASM_diskstring"consulte .

- Se você estiver criando o clone em um host alternativo, o host alternativo deverá atender aos seguintes requisitos:
  - O plug-in do SnapCenter para banco de dados Oracle deve ser instalado no host alternativo.
  - O host clone deve ser capaz de descobrir LUNs de storage primário ou secundário.
    - Se você estiver clonando do storage primário ou do storage secundário (Vault ou Mirror) para um host alternativo, certifique-se de que uma sessão iSCSI seja estabelecida entre o storage secundário e o host alternativo ou zoneada corretamente para FC.
    - Se você estiver clonando do armazenamento do Vault ou Mirror para o mesmo host, certifique-se de que uma sessão iSCSI seja estabelecida entre o armazenamento do Vault ou Mirror e o host, ou zoneada corretamente para o FC.
    - Se você estiver clonando em um ambiente virtualizado, certifique-se de que uma sessão iSCSI seja estabelecida entre o storage primário ou secundário e o servidor ESX que hospeda o host alternativo ou zoneada corretamente para o FC.

      Para obter informações, "documentação de utilitários do host" consulte .

  - Se o banco de dados de origem for um banco de dados ASM:
    - A instância 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 clone se você quiser colocar arquivos de log de arquivamento do banco de dados clonados 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 o clone será executado.

      Os arquivos de dados que residem no grupo de discos ASM são provisionados como parte do fluxo de trabalho do clone do SnapCenter.

  - Para NVMe, o NVMe útil deve ser instalado
- O tipo de proteção para o LUN de dados e o LUN de log, como espelho, cofre ou espelho-Vault, 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 parâmetro do banco de dados de origem para recuperar informações relacionadas ao PDB de semente para clonar um backup do banco de dados 12_c_.

  A PDB de semente é um modelo fornecido pelo sistema que o CDB pode usar para criar PDBs. O PDB de semente é chamado de PDB DE SEMENTE. Para obter informações sobre o PDB, 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, verifique se os pontos de montagem de dados não estão sob a raiz do ponto de montagem do autofs porque o usuário raiz do host do plug-in não tem permissão para criar diretórios sob a raiz do ponto de montagem do autofs.

  Se os arquivos de log de controle e refazer estiverem sob ponto de montagem de dados, você deve modificar o caminho do arquivo de controle e refazer o caminho do arquivo de log de acordo.

  Você pode Registrar manualmente os novos pontos de montagem clonados com o subsistema autofs. Os novos pontos de montagem clonados não serão registados automaticamente.

- Se você tiver um TDE (login automático) e quiser clonar o banco de dados no mesmo host ou alternativo, copie 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 a clonagem com sucesso em ambientes de rede de área de armazenamento (SAN) no Oracle Linux 7 ou posterior ou Red Hat Enterprise Linux (RHEL) 7 ou posterior.
- Você deve instalar o patch 13366202 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 storage (SVM).
- Para NVMe, se qualquer 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 criar o arquivo como 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 seja mapeado para o host AIX usando o iGroup que consiste em protocolos mistos iSCSI e FC. Para obter mais informações, "A operação falha com erro não é possível descobrir o dispositivo para LUN"consulte .

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 tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios prescritor 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 refazer on-line e arquivos de controle. O banco de dados pode ser recuperado opcionalmente para um tempo especificado, 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 autônomo quando clonado a partir de um backup de banco de dados do Oracle RAC. O SnapCenter suporta a criação de clone a partir do backup de bancos de dados em espera do Data Guard e do ative Data Guard.

  Durante a clonagem, o SnapCenter monta o número ideal de backups de log com base em SCN ou dat e tempo para operações de recuperação. Após a recuperação, o backup de log é desmontado. Todos esses clones são montados em */var/opt/SnapCenter/scu/clones/*. Se você estiver usando ASM em 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 clone em Leaf Nodes se a cardinalidade for menor que os nós numéricos no cluster RAC.

- Para políticas habilitadas para o SnapLock, para ONTAP 9.12,1 e versões abaixo, se você especificar um período de bloqueio do Snapshot, os clones criados a partir dos snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 de cópias locais (primárias), cópias espelhadas (secundárias) ou cópias do Vault (secundárias).
5. Selecione a cópia de segurança de dados na tabela e, em seguida, 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 tamanho máximo do SID é de 8 carateres. Você deve garantir que nenhum banco de dados com o mesmo SID exista no host onde o clone será criado.
Clonar um banco de dados conetável (PDB)	a. Selecione **Clonar PDB**. b. Especifique o PDB que você deseja clonar. c. Especifique o nome do PDB clonado. Para obter as etapas detalhadas para clonar um PDB, "Clone um banco de dados conetável"consulte .

Quando você seleciona um dado espelhado ou de cofre:

- se não houver backup de log no mirror ou vault, nada será selecionado e os localizadores estarão vazios.
- se existirem cópias de segurança de registo no mirror ou no vault, a cópia de segurança de registo mais recente é selecionada e o localizador correspondente é apresentado.

Se a cópia de segurança de registo selecionada existir na localização do espelho e do cofre, ambos os localizadores são apresentados.

7. Na página locais, execute as seguintes ações:

Para este campo…	Faça isso…
Clone de host	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 com a mesma versão do Oracle e do SO que o host do banco de dados de origem.

Para este campo…	Faça isso…
Localizações de ficheiros de dados	Por padrão, a localização do arquivo de dados é preenchida. 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 adere ao comprimento máximo suportado pela Oracle. Se você quiser especificar um caminho diferente, insira os pontos de montagem do arquivo de dados ou nomes de grupo de discos ASM para o banco de dados clone. Ao personalizar o caminho do arquivo de dados, você também deve alterar o arquivo de controle e refazer os nomes de grupo de discos ASM do arquivo de log ou sistema de arquivos para o mesmo nome usado para arquivos de dados ou para um grupo de discos ASM existente ou sistema de arquivos.

Para este campo…	Faça isso…
Controlar ficheiros	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 que os arquivos de dados. Se você 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 um mínimo de um arquivo de controle é necessário para clonar o banco de dados. Você pode personalizar o caminho do arquivo de controle para um sistema de arquivos diferente (existente) do banco de dados de origem.

Para este campo…	Faça isso…
Refazer registos	Por padrão, o grupo de arquivos de log refazer, o caminho e seus tamanhos são preenchidos. Os logs de refazer são colocados no mesmo grupo de discos ASM ou sistema de arquivos que os arquivos de dados do banco de dados clonado. Se você quiser substituir o caminho do arquivo de log de refazer, você pode personalizar o caminho do arquivo de log de refazer para um sistema de arquivos diferente 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 log refazer, refazer arquivos de log e seus tamanhos serão os mesmos do banco de dados de origem. Você pode modificar os seguintes parâmetros: • Número de grupos de registo refazer ⓘ É necessário um mínimo de dois grupos de log de refazer para clonar o banco de dados. • Refaça os 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) do banco de dados de origem. ⓘ Um mínimo de um arquivo de log de refazer é necessário no grupo de log de refazer para clonar o banco de dados. • Tamanhos do ficheiro de registo de refazer

8. Na página credenciais, execute as seguintes ações:

Para este campo…	Faça isso…
Nome da credencial para o usuário do sistema	Selecione a credencial a ser usada para definir a senha do usuário do sistema do banco de dados clone. Se SQLNET.AUTHENTICATION_SERVICES estiver definido como NONE no arquivo sqlnet.ora no host de destino, você não deve selecionar **None** como credencial na GUI do SnapCenter.
Nome da credencial da instância ASM	Selecione **nenhum** se a autenticação do sistema operacional estiver ativada para conexão com a instância ASM no host clone. Caso contrário, selecione a credencial Oracle ASM configurada com o usuário "s" ou um usuário com privilégio "sysasm" aplicável ao host clone.

A casa, o nome de usuário e os detalhes do grupo do Oracle 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 do prescritor que você deseja executar antes da operação clone.

      Você deve armazenar o prescritor 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 é colocado.

      O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript. "Saiba 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.

      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 do log de reprocessamento de arquivo, adicione os parâmetros e especifique o caminho.

      - LOG_ARCHIVE_DEST
      - LOG_ARCHIVE_DUPLEX_DEST

      > A área de recuperação rápida (FRA) não está definida nos parâmetros do banco de dados pré-preenchidos. Você pode configurar FRA adicionando os parâmetros relacionados.

O valor padrão de log_archive_dest_1 é ORACLE_Home/clone_sid e os logs de arquivo do banco de dados clonados serão criados nesse local. Se você tiver excluído o parâmetro log_archive_dest_1, o local do log do arquivo será determinado pela Oracle. Você pode definir um novo local para o log de arquivo editando log_archive_dest_1, mas certifique-se de que o sistema de arquivos ou o grupo de discos deve estar existente e disponibilizado no host.

a. Clique em **Reset** para obter as configurações padrão de parâmetros do banco de dados.

10. Na página PostOps, **Recover database** e **Until Cancel** 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 storage primário para executar o clone no storage primário e o backup de dados deve estar no storage secundário para executar o clone no storage secundário.

    As opções **Recover database** e **Until Cancel** não são selecionadas se o SnapCenter não conseguir encontrar os backups de log apropriados. Você pode fornecer o local de log de arquivamento externo se o backup de log não estiver disponível em **especificar locais de log de arquivamento externo**. Pode especificar vários locais de registo.

    Se você quiser clonar um banco de dados de origem configurado para suportar a área de recuperação flash (FRA) e os arquivos gerenciados Oracle (OMF), o destino do log para recuperação também deve aderir à estrutura de diretórios OMF.

    A página PostOps não será exibida se o banco de dados de origem for um banco de dados de espera do Data Guard ou um banco de dados de espera do ative Data Guard. Para o modo de espera do Data Guard ou um banco de dados em espera do ative Data Guard, o SnapCenter não fornece uma opção para selecionar o tipo de recuperação na GUI do SnapCenter, mas o banco de dados é recuperado usando até Cancelar o tipo de recuperação 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 arquivamento após esse 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 aceite é mm/dd/aaaa hh:mm:ss. A hora pode ser especificada no formato de 24 horas.
Até SCN (número de mudança do sistema)	O SnapCenter recupera o banco de dados até um número de mudança de sistema especificado (SCN).

Nome do campo	Descrição
Especifique locais de registo de arquivo externo	Se o banco de dados estiver sendo executado no modo ARCHIVELOG, o SnapCenter identifica e monta o número ideal de backups de log com base no SCN especificado ou na data e hora selecionadas. Também pode especificar a localização do registo de arquivo externo. O SnapCenter não identificará e montará automaticamente os backups de log se você tiver selecionado até Cancelar.
Crie um novo DBID	Por padrão **Create new DBID** caixa de seleção está selecionada para gerar um número único (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 com o catálogo RMAN externo onde o banco de dados de origem já está registrado, a operação falha.
Crie o tempfile para o espaço de tabela temporário	Marque a caixa de seleção se quiser criar um arquivo tempfile para o espaço de tabela temporário padrão do banco de dados clonado. Se a caixa de seleção não estiver selecionada, o clone do banco de dados será criado sem o tempfile.
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 serem executados após a operação clone	Especifique o caminho e os argumentos do postscript que você deseja executar após a operação clone. 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 é colocado. Se a operação de clone 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 quiser anexar o relatório da operação clone executada, 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-SmtpServer.

12. Revise o resumo e clique em **Finish**.

    Ao executar a recuperação como parte da operação de criação de clone, mesmo que a recuperação falhe, o clone é criado com um aviso. Você pode executar a recuperação manual neste clone para colocar o banco de dados clone no estado consistente.

13. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Resultado

Após a clonagem do banco de dados, você pode atualizar a página 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 ainda mais (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 pode falhar devido a uma recuperação inadequada, e talvez seja necessário executar a recuperação manual. O backup de log também pode falhar se o local padrão que foi preenchido para logs de arquivamento estiver em um armazenamento não NetApp ou se o sistema de armazenamento não estiver configurado com SnapCenter.

Na configuração 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.

O bloqueio ou a renomeação de dispositivos não afetará a operação de exclusão do clone. Para layouts de LVM AIX criados em dispositivos SAN, a renomeação de dispositivos não será suportada para os dispositivos SAN clonados.

Encontre mais informações

- "Falha na restauração ou clonagem com a mensagem de erro ORA-00308"
- "Falha ao recuperar um banco de dados clonado"
- "Parâmetros personalizáveis para operações de backup, restauração e clone em sistemas AIX"

Clone um banco de dados conetável

Você pode clonar um banco de dados conetável (PDB) para um CDB diferente ou mesmo destino no mesmo host ou host alternativo. Você também pode recuperar o PDB clonado para uma SCN ou data e hora desejadas.

Antes de começar

Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios prescritor e postscript.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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) 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 de cópias locais (primárias), cópias espelhadas (secundárias) ou cópias do Vault (secundárias).
5. Selecione a cópia de segurança na tabela e, em seguida, clique em * .
6. Na página Nome, execute as seguintes ações:
   a. Selecione **Clonar PDB**.
   b. Especifique o PDB que você deseja clonar.

      Você pode clonar apenas um PDB de cada vez.

   c. Especifique o nome do clone PDB.
7. Na página locais, execute as seguintes ações:

Para este campo…	Faça isso…

Clone de host	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 com a mesma versão do Oracle e do SO que o host do banco de dados de origem.
CDB alvo	Selecione o CDB onde deseja incluir o PDB clonado. Você deve garantir que o CDB alvo esteja em execução.
Estado da base de dados	Marque a caixa de seleção **abrir o PDB clonado no modo DE LEITURA-GRAVAÇÃO** se quiser abrir o PDB no modo DE LEITURA-GRAVAÇÃO.
Localizações de ficheiros de dados	Por padrão, a localização do arquivo de dados é preenchida. 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 adere ao comprimento máximo suportado pela Oracle. Se você quiser especificar um caminho diferente, insira os pontos de montagem do arquivo de dados ou nomes de grupo de discos ASM para o banco de dados clone.

A casa, o nome de usuário e os detalhes do grupo do Oracle 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 do prescritor que você deseja executar antes da operação clone.

      Você deve armazenar o prescritor 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 é colocado.

O SnapCenter permite-lhe utilizar as variáveis de ambiente predefinidas quando executa o prescritor e o postscript. "Saiba 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 **Reset** para obter as configurações padrão de parâmetros do banco de dados.
10. Na página PostOps, **Until Cancel** é selecionado por padrão para executar a recuperação do banco de dados clonado.

A opção **Until Cancel** (até Cancelar) não é selecionada se o SnapCenter não conseguir encontrar os backups de log apropriados. Você pode fornecer o local de log de arquivamento externo se o backup de log não estiver disponível em **especificar locais de log de arquivamento externo**. Pode especificar vários locais de registo.

Se você quiser clonar um banco de dados de origem configurado para suportar a área de recuperação flash (FRA) e os arquivos gerenciados Oracle (OMF), o destino do log para recuperação também deve aderir à estrutura de diretórios 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 esse backup de dados que foi selecionado para clonagem. O backup de log e dados deve estar no storage primário para executar o clone no storage primário e o backup de dados deve estar no storage secundário para executar o clone no storage 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. A hora pode ser especificada no formato de 24 horas.
Até SCN (número de mudança do sistema)	O SnapCenter recupera o banco de dados até um número de mudança de sistema especificado (SCN).
Especifique locais de registo de arquivo externo	Especifique a localização do log de arquivamento externo.

Nome do campo	Descrição
Crie um novo DBID	Por padrão **a caixa de seleção criar novo DBID** não está selecionada para o banco de dados de clones auxiliares. Marque a caixa de seleção se desejar gerar um número único (DBID) para o banco de dados clonado auxiliar diferenciando-o do banco de dados de origem.
Crie o tempfile para o espaço de tabela temporário	Marque a caixa de seleção se quiser criar um arquivo tempfile para o espaço de tabela temporário padrão do banco de dados clonado. Se a caixa de seleção não estiver selecionada, o clone do banco de dados será criado sem o tempfile.
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 serem executados após a operação clone	Especifique o caminho e os argumentos do postscript que você deseja executar após a operação clone. 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 é colocado. Se a operação de clone 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 quiser anexar o relatório da operação clone executada, 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-SmtpServer.

12. Revise o resumo e clique em **Finish**.

13. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Depois de terminar

Se você quiser criar um backup do PDB clonado, você deve fazer o backup do CDB de destino onde o PDB é clonado porque não é possível fazer backup apenas do PDB clonado. Você deve criar um relacionamento secundário para o CDB de destino se quiser criar o backup com relação secundária.

Em uma configuração RAC, o armazenamento para PDB clonado é anexado apenas ao nó onde o clone PDB foi executado. As PDBs nos outros nós do RAC estão no estado DE MONTAGEM. Se você quiser que o PDB clonado seja acessível a partir dos outros nós, anexe manualmente o storage aos outros nós.

Encontre mais informações

- "Falha na restauração ou clonagem com a mensagem de erro ORA-00308"
- "Parâmetros personalizáveis para operações de backup, restauração e clone em sistemas AIX"

Clonar backups de bancos de dados Oracle usando comandos UNIX

O fluxo de trabalho do clone inclui Planejamento, execução da operação do clone e monitoramento da operação.

Sobre esta tarefa

Você deve executar os seguintes comandos para criar o arquivo de especificação de clone de 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*. Em alternativa, pode também consultar o "Guia de Referência de comandos do software SnapCenter".

Passos

1. Crie uma especificação de clone de banco de dados Oracle a partir de um backup especificado: *New-SmOracleCloneSpecification*

   Se a política de proteção de dados secundária for unificada mirror-Vault, especifique somente -IncludeSecondaryDetails. Você não precisa especificar -SecondaryStorageType.

   Esse comando cria automaticamente um arquivo de especificação de clone de 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 estará criando.

   O arquivo de especificação do clone é criado em */var/opt/SnapCenter/SCO/clone_specs*.

2. Inicie uma operação de clone a partir de um grupo de recursos clone ou de um backup existente: *New-SmClone*

   Este comando inicia uma operação clone. Você também precisa 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 clone a ser executada, as prescrições, os postscripts 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_.

Divida 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 torna-se independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clones em um clone intermediário.

  Por exemplo, depois de criar clone1 a partir de um backup de banco de dados, você pode criar um backup de clone1 e clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e não é possível executar a operação de divisão de clones no clone1. No entanto, você pode executar a operação de divisão de clones no clone2.

  Depois de dividir clone2, você pode executar a operação de divisão de clones no clone1 porque clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup do clone são excluídas.
- Para obter informações sobre limitações de operação de divisão de clones, consulte "Guia de gerenciamento de storage lógico do ONTAP 9" .
- Certifique-se de que o volume ou o agregado no sistema de storage esteja on-line.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
5. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

   A operação de divisão de clones deixa de responder se o serviço SMCore for reiniciado e os bancos de dados nos quais a operação de divisão de clones foi executada são listados como clones na página recursos. Você deve executar o cmdlet *Stop-SmJob* para interromper a operação de divisão de clones e tentar novamente a operação de divisão de clones.

   Se você quiser um tempo de enquete mais longo 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 que o SMCore busque o status da operação de divisão de clones. O valor é em milissegundos e o valor padrão é de 5 minutos.

   Por exemplo,

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

A operação de inicialização dividida do clone falha se o backup, a restauração ou a divisão do clone do outro estiverem em andamento. Você deve reiniciar a operação de divisão de clones somente depois que as operações em execução estiverem concluídas.

Clone dividido de um banco de dados conetável

Você pode usar o SnapCenter para dividir um banco de dados conetável clonado (PDB).

Sobre esta tarefa

Se você criou um backup do CDB de destino onde o PDB é clonado, quando você divide 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 PDB não são exibidos na exibição de inventário ou recursos.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Selecione a base de dados de contentor de origem (CDB) na vista de grupo de recursos ou recursos.
3. Na exibição Gerenciar cópias, selecione **clones** nos sistemas de storage primário ou secundário (espelhado ou replicado).
4. Selecione o clone PDB (targetCDB:PDBClone) e clique em .
5. Revise o tamanho estimado do clone que deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Monitorar operações de clone de banco de dados Oracle

Você pode monitorar o andamento das operações de clone do SnapCenter usando a página tarefas. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.

2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista para que apenas operações de clone sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Atualize um clone

Você pode atualizar o clone executando o comando *Refresh-SmClone*. Esse 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 PDB.

O que você vai precisar

- Crie um backup completo online ou uma política de backup de dados offline sem backups programados ativados.
- Configure a notificação por e-mail na política apenas 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 apenas 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 clone de atualização.
- Crie um grupo de recursos com apenas um banco de dados.
- Se um cron job for criado para o comando clone refresh, certifique-se de que as programações do SnapCenter e as programações do cron não estejam sobrepostas 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 24hrs.

- Certifique-se de que o SID clone seja exclusivo para um host.

  Se várias operações de clone de atualização 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 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 do primário.

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado: *Open-SmConnection*
2. Crie uma especificação de clone de banco de dados Oracle a partir de um backup especificado: *New-SmOracleCloneSpecification*

   Se a política de proteção de dados secundária for unificada mirror-Vault, especifique somente -IncludeSecondaryDetails. Você não precisa especificar -SecondaryStorageType.

   Esse comando cria automaticamente um arquivo de especificação de clone de 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 estará criando.

   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: CanExecutar falha com erro: PL-SCO-30031: Refazer arquivo de log -SC_2959770772_clmdb/clmdb/redolog/redo01_01.log exists", especifique um valor mais alto para *-WaitToTriggerClone*.

   Para obter informações detalhadas sobre comandos UNIX, consulte "Guia de Referência de comandos do software SnapCenter" .

Excluir clone de um banco de dados conetável

Você pode excluir o clone de um banco de dados conetável (PDB) se não precisar mais.

Se você criou um backup do CDB de destino onde o PDB é clonado, quando você exclui o clone do PDB, o PDB clonado também é removido do backup do CDB de destino.

Os clones PDB não são exibidos na exibição de inventário ou recursos.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Selecione a base de dados de contentor de origem (CDB) na vista de grupo de recursos ou recursos.
3. Na exibição Gerenciar cópias, selecione **clones** nos sistemas de storage primário ou secundário (espelhado ou replicado).
4. Selecione o clone PDB (targetCDB:PDBClone) e clique em .
5. Clique em **OK**.

Gerenciar volumes de aplicações

O que são volumes de aplicações

Volumes de aplicativos são o armazenamento onde informações como configuração, instalador e outros arquivos não relacionados a banco de dados Oracle são armazenados.

O plug-in do SnapCenter para banco de dados Oracle permite criar backup consistente 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 aplicações.

- Proteja volumes de aplicações juntamente com volumes de banco de dados Oracle em um único grupo de recursos.
- Criar backups de volumes de aplicações.
- Crie backups de bancos de dados Oracle junto com volumes de aplicações.
- Crie clones de bancos de dados e volumes de aplicações em um ponto no tempo.
- Agendar operações de backup.
- Monitorar todas as operações.
- Exibir relatórios de operações de backup e clone.

Adicionar volumes de aplicações

O SnapCenter é compatível com backup e clonagem de volumes de aplicações de banco de dados Oracle. Você deve adicionar manualmente os volumes de aplicativos. A deteção automática de volumes de aplicações não é suportada.

Os volumes de aplicações são compatíveis apenas com conexões diretas NFS e iSCSI.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.
2. Clique em **Add Application volume** (Adicionar volume da aplicação).
3. Na página Nome, execute as seguintes ações:
   - No campo Nome , introduza o nome do volume da aplicação.
   - No campo Nome do host , digite o nome do host.
4. Na página espaço físico do armazenamento, insira o nome do sistema de armazenamento, selecione um ou volumes e especifique os LUNs ou Qtrees associados.

   Você pode adicionar vários sistemas de storage.
5. Revise o resumo e clique em **Finish**.
6. Na página recursos, selecione **volume do aplicativo** na lista **Exibir** para exibir todos os volumes de aplicativos adicionados.

Modificar o volume da aplicação

Você pode modificar todos os valores especificados ao adicionar o volume do aplicativo, se não forem criados backups. Se o backup for criado, você só poderá modificar os detalhes do sistema de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.
2. Na página recursos, selecione **volume do aplicativo** na lista **Exibir**.
3. Clique em para modificar os valores.

Eliminar volume da aplicação

Quando você exclui um volume de aplicativo, se houver backups associados ao volume do aplicativo, o volume do aplicativo será colocado em 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 anular a operação de eliminação.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.
2. Na página recursos, selecione **volume do aplicativo** na lista **Exibir**.
3. Clique em para modificar os valores.

Volumes de aplicações de backup

Fazer backup do volume do aplicativo

Se o volume do aplicativo não fizer parte de qualquer grupo de recursos, você poderá fazer backup do volume do aplicativo na página recursos.

Sobre esta tarefa

Por padrão, backups do grupo de consistência (CG) são criados. Se você quiser criar backups baseados em volume, defina o valor de **EnableOracleNdvVolumeBasedBackup** como verdadeiro no arquivo *web.config*.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.
2. Na página recursos, selecione **volume do aplicativo** na lista **Exibir**.
3. Clique em e selecione o nome do host e o tipo de banco de dados para filtrar os recursos.

   Em seguida, pode clicar para fechar o painel de filtro.

4. Selecione o volume da aplicação que pretende efetuar uma cópia de segurança.

   É apresentada a página de proteção do volume da aplicação.

5. Na página recurso, execute as seguintes ações:

Para este campo…	Faça isso…
Use o formato de nome personalizado para cópia Snapshot	Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea. Por exemplo, customtext__policy_hostname ou resource_hostname. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.
Excluir destinos de log de arquivamento do backup	Especifique os destinos dos ficheiros de registo de arquivo que não pretende efetuar uma cópia de segurança.

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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

   c. Na janela Adicionar programações para a política *policy_name*, configure a programação e clique em **OK**.

      policy_name é o nome da política selecionada.

   As programações configuradas são listadas na coluna agendas aplicadas.

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 e 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-SmtpServer.

8. Revise o resumo e clique em **Finish**.

   É apresentada a página topologia do volume da aplicação.

9. Clique em **fazer backup agora**.
10. Na página Backup, execute as seguintes etapas:

    a. Se você tiver aplicado várias políticas ao recurso, na lista suspensa **Política**, selecione a política que deseja usar para backup.

b. Clique em **Backup**.

11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Faça backup do grupo de recursos volumes de aplicativos

É possível fazer backup do grupo de recursos que contém apenas volumes de aplicativos ou uma combinação 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 aplicações, todos os volumes de aplicações deverão ter uma política de replicação do SnapMirror ou do SnapVault.

Sobre esta tarefa

Por padrão, backups do grupo de consistência (CG) são criados. Se você quiser criar backups baseados em volume, defina o valor de **EnableOracleNdvVolumeBasedBackup** como verdadeiro no arquivo *web.config*.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in 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 selecionando a tag. Em seguida, pode clicar para fechar o painel de filtro.

3. Na página grupos de recursos, selecione o grupo de recursos que deseja fazer backup e clique em **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. Clique em **Backup**.
5. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

> A operação de verificação será realizada apenas para os bancos de dados e não para os volumes de aplicativos.

Clone o backup de volume de aplicativo

Você pode usar o SnapCenter para clonar os backups de volume de aplicações.

Antes de começar

Se tiver instalado o plug-in como um utilizador não root, deve atribuir manualmente as permissões de execução aos diretórios prescritor e postscript.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in Oracle Database na lista.
2. Na página recursos, selecione **volume do aplicativo** na lista **Exibir**.
3. Selecione o volume da aplicação na vista de detalhes do volume da aplicação ou na vista de detalhes do grupo de recursos.

   É apresentada a página topologia do volume da aplicação.

4. Na exibição Gerenciar cópias, selecione os backups de cópias locais (primárias), cópias espelhadas (secundárias) ou cópias do Vault (secundárias).
5. Selecione a cópia de segurança na tabela e, em seguida, clique em * .
6. Na página localização, execute as seguintes ações:

Para este campo…	Faça isso…
Host plug-in	Selecione o host onde você deseja criar o clone.
Nome recurso alvo	Especifique o nome do recurso.

7. Na página Scripts, especifique os nomes dos scripts a serem executados antes da clonagem, comandos para montar um sistema de arquivos e 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 quiser anexar o relatório da operação clone executada, 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-SmtpServer.

9. Revise o resumo e clique em **Finish**.

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 torna-se independente do recurso pai.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in 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 deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
5. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Excluir um clone de volume de aplicativo

Você pode excluir clones se você achar que eles não são mais necessários. Não é possível excluir clones que atuam como fonte para outros clones.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in 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** nos sistemas de storage 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 **Pré-clone delete**, insira os nomes dos scripts a serem executados antes de excluir o clone.
   b. No campo **Desmontar**, digite os comandos para desmontar o clone antes de excluir o clone.
7. Clique em **OK**.

Proteja os sistemas de arquivos do Windows

Plug-in do SnapCenter para conceitos do Microsoft Windows

Visão geral do plug-in do SnapCenter para Microsoft Windows

O plug-in do SnapCenter para Microsoft Windows é um componente do lado do host do software NetApp SnapCenter que permite o gerenciamento de proteção de dados com reconhecimento de aplicativos dos recursos do sistema de arquivos da Microsoft. Além disso, ele fornece provisionamento de storage, consistência Snapshot e recuperação de espaço para sistemas de arquivos Windows. O plug-in para Windows automatiza as operações de backup, restauração e clonagem do sistema de arquivos em seu ambiente SnapCenter.

Quando o plug-in para Windows é instalado, você pode usar a tecnologia SnapCenter com NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia NetApp SnapVault para executar replicação de backup disco a disco para conformidade de arquivamento ou padrões.

O que você pode fazer com o plug-in SnapCenter para Microsoft Windows

Quando o plug-in para Windows está instalado no seu ambiente, você pode 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
- Faça backup dos sistemas de arquivos do Windows
- Agendar operações de backup
- Restaure backups do sistema de arquivos
- Clonar backups do sistema de arquivos
- Monitore operações de backup, restauração e clone

O plug-in para Windows não suporta backup e restauração de sistemas de arquivos em compartilhamentos SMB.

Plug-in do SnapCenter para recursos do Windows

O plug-in para Windows se integra à tecnologia Snapshot do NetApp no sistema de storage. Para trabalhar com o plug-in para Windows, use a interface SnapCenter.

O plug-in para Windows inclui estes principais recursos:

- * Interface gráfica unificada do usuário com SnapCenter*

  A interface do SnapCenter fornece padronização e consistência entre plug-ins e ambientes. A interface do SnapCenter permite concluir processos consistentes de backup e restauração em plug-ins, usar relatórios

centralizados, usar visualizações de dashboard rápidas, configurar controle de acesso baseado em funções (RBAC) e monitorar tarefas em todos os plug-ins. O SnapCenter também oferece gerenciamento centralizado de políticas e agendamento para dar suporte a operações de backup e clone.

- * Administração central automatizada*

  Você pode agendar backups de rotina do sistema de arquivos, configurar a retenção de backup baseada em política e configurar operações de restauração. Você também pode monitorar proativamente o ambiente do sistema de arquivos configurando o SnapCenter para enviar alertas por e-mail.

- **Tecnologia NetApp Snapshot sem interrupções**

  O plug-in para Windows usa a tecnologia Snapshot do NetApp. Isso permite que você faça backup de sistemas de arquivos em segundos e restaurá-los rapidamente sem deixar o host off-line. Os snapshots consomem espaço mínimo de storage.

Além desses principais recursos, o plug-in para Windows oferece os seguintes benefícios:

- Suporte ao fluxo de trabalho de backup, restauração e clone
- Delegação de funções centralizada e segurança compatível com RBAC
- Criação de cópias com uso eficiente de espaço de sistemas de arquivos de produção para teste ou extração de dados usando a tecnologia NetApp FlexClone

  Para obter informações sobre licenciamento do FlexClone, "Licenças SnapCenter"consulte .

- Capacidade de executar vários backups ao mesmo tempo em vários servidores
- Cmdlets do PowerShell para scripts de operações de backup, restauração e clone
- Suporte para backup de sistemas de arquivos e discos de máquina virtual (VMDKs)
- Suporte para infraestruturas físicas e virtualizadas
- Suporte para iSCSI, Fibre Channel, FCoE, mapeamento de dispositivo bruto (RDM), mapeamento LUN assimétrico (ALM), VMDK sobre NFS e VMFS e FC virtual
- Suporte para memória não volátil Express (NVMe) no Windows Server 2022
  - Workflows de backup, restauração, clone e verificação no layout VMDK criado no NVMe em TCP/IP.
  - Suporta a versão 1,3 do firmware NVMe a partir da atualização 2 do ESX 8,0 e requer a versão 21 do hardware virtual.
  - O WSFC (Cluster de failover do Windows Server) não é compatível com aplicativos em VMDK em NVMe em TCP/IP.
- É compatível com a sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), que permite que os serviços empresariais continuem operando mesmo em caso de falha completa do local, oferecendo suporte para failover transparente de aplicações usando uma cópia secundária. Nem a intervenção manual nem o script adicional são necessários 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 dos 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 snapshots dos sistemas de arquivos. Os backups federados, em que um volume contém LUNs de vários hosts, são mais rápidos e eficientes do que os 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 instantâneo, todo o volume do sistema de storage é capturado no instantâneo. No entanto, o backup é válido apenas para o servidor host para o qual o backup foi criado.

Se os dados de outros servidores host residirem no mesmo volume, esses dados não poderão ser restaurados a partir do Snapshot.

Se um sistema de arquivos do Windows contiver um banco de dados, o backup do sistema de arquivos não será o mesmo que o backup do banco de dados. Para fazer backup de um banco de dados, você deve usar um dos plug-ins do banco de dados.

Tipos de storage compatíveis com o plug-in SnapCenter para Microsoft Windows

O SnapCenter suporta uma ampla variedade de tipos de armazenamento em máquinas físicas e máquinas virtuais. Você deve verificar se há suporte disponível para o seu tipo de armazenamento antes de instalar o pacote para o seu host.

O suporte para provisionamento e proteção de dados do SnapCenter está disponível no Windows Server. Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Máquina	Tipo de armazenamento	Provisione usando	Notas de suporte
Servidor físico	LUNs conectados a FC	Cmdlets da interface gráfica do usuário (GUI) do SnapCenter ou do PowerShell	
Servidor físico	LUNs ligados ao iSCSI	Cmdlets SnapCenter GUI ou PowerShell	
Servidor físico	Compartilhamentos de SMB3 TB (CIFS) residentes em uma máquina virtual de storage (SVM)	Cmdlets SnapCenter GUI ou PowerShell	Suporte apenas para provisionamento.
VMware VM	LUNs RDM ligados por um FC ou iSCSI HBA	Cmdlets do PowerShell	

Máquina	Tipo de armazenamento	Provisione usando	Notas de suporte
VMware VM	ISCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets SnapCenter GUI ou PowerShell	
VMware VM	Armazenamentos de dados NFS ou VMFS (Virtual Machine File Systems)	VMware vSphere	
VMware VM	Um sistema convidado conetado a SMB3 compartilhamentos residentes em um SVM	Cmdlets SnapCenter GUI ou PowerShell	Suporte apenas para provisionamento.
VMware VM	Armazenamentos de dados da VVol em NFS e SAN	Ferramentas do ONTAP para VMware vSphere	
VM Hyper-V	LUNs de FC virtual (VFC) conectados por um switch Fibre Channel virtual	Cmdlets SnapCenter GUI ou PowerShell	Você deve usar o Hyper-V Manager para provisionar LUNs Virtual FC (VFC) conectados por um switch Fibre Channel virtual. O Hyper-V passa por discos e faz backup de bancos de dados em VHD(x) que são provisionados no armazenamento NetApp não são suportados.

Máquina	Tipo de armazenamento	Provisione usando	Notas de suporte
VM Hyper-V	ISCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets SnapCenter GUI ou PowerShell	O Hyper-V passa por discos e faz backup de bancos de dados em VHD(x) que são provisionados no armazenamento NetApp não são suportados.
VM Hyper-V	Um sistema convidado conetado a SMB3 compartilhamentos residentes em um SVM	Cmdlets SnapCenter GUI ou PowerShell	Suporte apenas para provisionamento. O Hyper-V passa por discos e faz backup de bancos de dados em VHD(x) que são provisionados no armazenamento NetApp não são suportados.

ONTAP Privileges mínimo necessário para o plug-in do Windows

Os ONTAP Privileges mínimos necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
  - event generate-AutoSupport-log
  - mostra o histórico de trabalhos
  - paragem do trabalho
  - lun
  - lun criar

- eliminação lun
- lun igrop add
- lun igrop criar
- eliminação do agrupamento lun
- mudar o nome do grupo lun
- show de grupos de lun
- nós complementares de mapeamento de lun
- mapeamento lun criar
- eliminação do mapeamento lun
- mapeamento lun remove-reporting-nonos
- mostra de mapeamento lun
- modificação de lun
- movimentação de lun no volume
- lun offline
- lun online
- redimensionar lun
- série lun
- mostra lun
- regra adicional de política do SnapMirror
- regra de modificação de política do SnapMirror
- regra de remoção da política do SnapMirror
- SnapMirror policy show
- restauração de SnapMirror
- SnapMirror show
- SnapMirror show-history
- atualização do SnapMirror
- SnapMirror update-ls-set
- SnapMirror lista-destinos
- versão
- clone de volume criar
- show de clone de volume
- início da divisão do clone de volume
- paragem dividida clone volume
- criar volume
- destruição de volume
- clone de arquivo de volume criar
- show-disk-use do arquivo de volume

    - volume off-line
    - volume online
    - modificação do volume
    - criar qtree de volume
    - eliminação de qtree de volume
    - modificação de qtree de volume
    - apresentação de qtree de volume
    - restrição de volume
    - apresentação do volume
    - criar instantâneo de volume
    - eliminar instantâneo do volume
    - modificação do instantâneo do volume
    - mudar o nome do instantâneo do volume
    - restauração de snapshot de volume
    - restauração de arquivo de snapshot de volume
    - apresentação de instantâneo do volume
    - desmontar o volume
    - svm cifs
    - compartilhamento cifs de svm criar
    - exclusão de compartilhamento cifs de svm
    - apresentação do shadowcopy cifs de svm
    - exibição de compartilhamento cifs de svm
    - mostra cifs de svm
    - política de exportação de svm
    - criação de política de exportação de svm
    - exclusão da política de exportação do svm
    - regra de política de exportação de svm criar
    - a regra de política de exportação do svm é exibida
    - exibição da política de exportação do svm
    - svm iscsi
    - apresentação da ligação iscsi de svm
    - mostra o svm
- Comandos somente leitura: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
    - interface de rede
    - mostra da interface de rede
    - svm

Preparar sistemas de storage para replicação SnapMirror e SnapVault

Você pode usar um plug-in do 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 disco a disco para conformidade com os padrões e outros fins relacionados à governança. Antes de executar essas tarefas, você deve configurar uma relação de proteção de dados entre os volumes de origem e destino e inicializar a relação.

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 . Se você estiver usando a sincronização ativa do SnapMirror , use os agendamentos padrão do SnapMirror ou SnapVault para a sincronização ativa do SnapMirror e para relacionamentos assíncronos.

Se você estiver vindo para o SnapCenter de um produto NetApp SnapManager e estiver satisfeito com as relações de proteção de dados que configurou, ignore esta seção.

Uma relação de proteção de dados replica dados no storage primário (o volume de origem) para o storage secundário (o volume de destino). Ao inicializar a relação, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não suporta relações em cascata entre volumes SnapMirror e SnapVault (**Primary** > **Mirror** > **Vault**). Você deve usar relacionamentos de fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis de versão e como configurá-los, consulte "Documentação do ONTAP".

Definir uma estratégia de backup para sistemas de arquivos do Windows

A definição de uma estratégia de backup antes de criar seus backups fornece os backups de que você precisa para restaurar ou clonar com sucesso seus sistemas de arquivos. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (rto) e objetivo do ponto de restauração (RPO) determinam em grande parte a sua estratégia de backup.

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. Rto é o momento em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a era dos arquivos que precisam 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.

Agendas de backup para sistemas de arquivos do Windows

A frequência de backup é especificada em políticas; uma programação de backup é especificada na configuração do grupo de recursos. O fator mais crítico na determinação de uma 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 usado a cada hora, enquanto você pode fazer backup de um recurso raramente usado uma vez por dia. Outros fatores incluem a importância do recurso para a sua organização, seu Contrato de nível de Serviço (SLA) e seu objetivo de ponto de recuperação (RPO).

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. Um RPO define a estratégia para a era dos arquivos que precisam ser recuperados do storage 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 usado, não é necessário executar um backup completo mais de uma ou duas vezes por dia.

Os programas de backup têm duas partes, como segue:

- Frequência de backup

  A frequência de backup (com que frequência os backups devem ser executados), chamada *schedule type* para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como hora, dia, semanal ou mensal, ou pode especificar **nenhum**, o que torna a política uma política somente sob demanda. Você pode acessar políticas clicando em **Configurações** > **políticas**.

- Fazer backup de programações

  As agendas 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 que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas. Você pode acessar programações de 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 de que você precisa 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 carimbo de data/hora aos nomes de Snapshot 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. Em contraste, se você quiser usar uma convenção de nomenclatura de backup personalizada, você precisa

renomear o backup após a conclusão da operação de backup.

Opções de retenção de backup

Você pode escolher o número de dias para os quais reter cópias de backup ou especificar o número de cópias de backup que deseja reter, até um máximo de ONTAP de 255 cópias. Por exemplo, sua organização pode exigir que você retenha 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 tiver sido alterado para o grupo de recursos ou recursos, os backups com o rótulo de tipo de agendamento antigo ainda poderão permanecer no sistema.

Para retenção de longo prazo de cópias de backup, você deve usar o backup SnapVault.

Fontes e destinos de clones para sistemas de arquivos do Windows

Você pode clonar um backup de sistema de arquivos do storage primário ou do storage secundário. Você também pode escolher o destino que atende aos seus requisitos: 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.

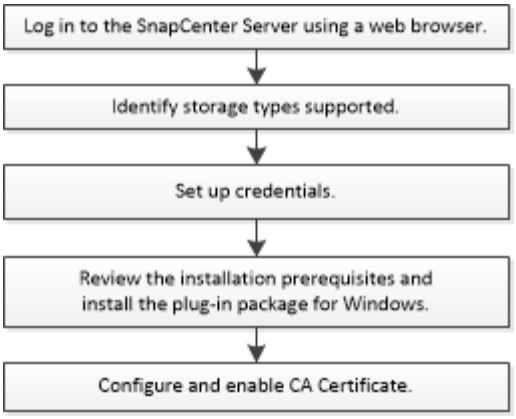
Destino do clone	Descrição
Original, origem, localização	Por padrão, o SnapCenter armazena o clone no mesmo local e no mesmo host que o backup sendo clonado.
Localização diferente	Você pode armazenar o clone em um local diferente no mesmo host ou em um host diferente. O host deve ter uma conexão configurada com a máquina virtual de storage (SVM).

Você pode renomear o clone depois que a operação de clone estiver concluída.

Instale o plug-in do SnapCenter para Microsoft Windows

Fluxo de trabalho de instalação do plug-in SnapCenter para Microsoft Windows

Você deve instalar e configurar o plug-in do SnapCenter para Microsoft Windows se quiser proteger arquivos do Windows que não sejam arquivos de banco de dados.



Requisitos de instalação para o 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 servidor SnapCenter e executar tarefas pré-requisitos.

- Você deve ter o SnapCenter admin Privileges para instalar o plug-in para Windows.

  A função de administrador do SnapCenter deve ter admin Privileges.

- Você deve ter instalado e configurado o servidor SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar 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 do 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 do sistema host e requisitos de dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do 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

Item	Requisitos
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• .NET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell Core 7.4.2 Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade 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 a instalação de 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 os plug-ins.
- Você deve configurar as credenciais com o Privileges de administrador, incluindo direitos de administrador, no host remoto.
- Se você configurar credenciais para grupos de recursos individuais e o usuário não tiver Privileges de administrador completo, será necessário atribuir ao usuário pelo menos o grupo de recursos e Privileges de backup.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Clique em **novo**.
4. Na página Credential (credencial), faça o seguinte:

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para as credenciais.
Nome de utilizador/Palavra-passe	Introduza o nome de utilizador e a palavra-passe utilizados 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 no qual você está instalando o plug-in do SnapCenter. Os formatos válidos para o campo Nome de usuário são os seguintes: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` ◦ `UserName@upn` • Administrador local (apenas para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é o seguinte: `UserName` Não use aspas duplas (") ou backtick (') nas senhas. Você não deve usar os símbolos menos de (>) e exclamação (!) juntos em senhas. Por exemplo, lessthan!10, lessthan10You!, backtick'12.
Palavra-passe	Introduza a palavra-passe utilizada 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.

Configure o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite criar uma conta de serviço gerenciado de grupo (gMSA) que fornece gerenciamento automatizado de senha de conta de serviço a partir de uma conta de domínio gerenciado.

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 é um membro do domínio.

Passos

1. Crie uma chave raiz KDS para gerar senhas exclusivas para cada objeto em seu gMSA.
2. Para cada domínio, execute o seguinte comando do 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,…>
.. Execute `Get-ADServiceAccount` o comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Ative o módulo do ative Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando do 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 o host.

b. Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua o Privileges administrativo ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no servidor SnapCenter.

   O servidor SnapCenter 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.

Adicione hosts e instale o plug-in do SnapCenter para Microsoft Windows

Você pode usar a página Adicionar host do SnapCenter para adicionar hosts do Windows. O plug-in do 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 para um cluster.

Antes de começar

- Se o sistema operacional do host do servidor SnapCenter for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deve executar o seguinte:
  - Atualize para o Windows Server 2019 (versão de SO 17763,5936) ou posterior
  - Atualize para o Windows Server 2022 (versão de SO 20348,2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o

UAC no host.

- O usuário do SnapCenter deve ser adicionado à função "Iniciar sessão como um serviço" do Windows Server.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja no estado em execução.
- Se você estiver usando a conta de serviço gerenciado de grupo (gMSA), você deve configurar o gMSA com Privileges administrativo.

  "Configure a conta de serviço gerenciado de grupo no Windows Server 2016 ou posterior para o sistema de arquivos do Windows"

Sobre esta tarefa

- Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.
- Plug-ins do Windows
  - Microsoft Windows
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
- Instalar 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 e-Series

  Não é possível instalar o plug-in para Windows em um host do Windows conetado ao armazenamento do e-Series.

O SnapCenter não suporta a adição do mesmo host (host plug-in) ao SnapCenter se o host já faz parte de um grupo de trabalho e foi alterado para outro domínio ou vice-versa. Se você quiser adicionar o mesmo host, remova o host do SnapCenter e adicione-o 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 **Add**.
4. Na página hosts, faça o seguinte:

Para este campo…	Faça isso…
Tipo de host	Selecione o tipo de host **Windows**. O servidor SnapCenter adiciona o host e, em seguida, instala o plug-in para Windows se ele ainda não estiver instalado no host.

Para este campo…	Faça isso…
Nome do host	Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada 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: • Anfitrião independente • Cluster de failover do Windows Server (WSFC) Se você estiver adicionando um host usando o SnapCenter e fizer parte de um subdomínio, você deverá fornecer o FQDN.
Credenciais	Selecione o nome da credencial que você criou ou crie as novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte informações sobre como criar uma credencial. Os detalhes sobre as credenciais, incluindo o nome de usuário, domínio e tipo de host, são exibidos colocando o cursor sobre o nome da credencial fornecida. 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 instalar.

   Para novas implantações, nenhum pacote de plug-in está listado.

6. (Opcional) clique em **mais opções**.

Para este campo…	Faça isso…
Porta	Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido 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, você deve especificar a mesma porta. Caso contrário, a operação falha.
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 do SnapCenter para Windows, o caminho padrão é C: Arquivos de programas/NetApp/SnapCenter. No entanto, se quiser, você pode personalizar o caminho padrão.
Adicione todos os hosts no cluster	Marque essa caixa de seleção para adicionar todos os nós de cluster em um WSFC.
Ignorar as verificações de pré-instalação	Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	Marque essa caixa de seleção se quiser usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in. Forneça o nome gMSA no seguinte formato: _Domainname O gMSA será usado como uma conta de serviço de logon apenas para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

Se você não selecionou 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 o local são validados de acordo com os requisitos mínimos. Se os requisitos mínimos não forem cumpridos, são apresentadas mensagens de erro ou de aviso adequadas.

Se o erro estiver relacionado ao espaço em disco ou à RAM, você poderá atualizar o arquivo web.config localizado no `C:\Program Files\NetApp\SnapCenter` WebApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.

> Em uma configuração de HA, se você estiver atualizando o arquivo web.config, será necessário atualizar o arquivo em ambos os nós.

8. Monitorize o progresso da instalação.

Instale o plug-in do SnapCenter para Microsoft Windows em vários hosts remotos usando cmdlets do PowerShell

Se você quiser instalar o plug-in do SnapCenter para Microsoft Windows em vários hosts ao mesmo tempo, use o `Install-SmHostPackage` cmdlet do PowerShell.

Você deve ter feito 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 servidor SnapCenter, estabeleça uma sessão usando `Open-SmConnection` o cmdlet e insira suas credenciais.
3. Adicione o host autônomo ou o cluster ao SnapCenter usando `Add-SmHost` o 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

4. Instale o plug-in em vários hosts usando `Install-SmHostPackage` o cmdlet e os parâmetros necessários.

   Você pode usar a `-skipprecheck` opção quando tiver instalado os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

Instale o plug-in do SnapCenter para Microsoft Windows silenciosamente a partir da linha de comando

Você pode instalar o plug-in do SnapCenter para Microsoft Windows localmente em um host do Windows se não conseguir instalar o plug-in remotamente a partir da GUI do SnapCenter. Você pode executar o plug-in do SnapCenter para o programa de instalação do Microsoft Windows sem supervisão, no modo silencioso, a partir da linha de comando do Windows.

Antes de começar

- Você deve ter instalado o Microsoft .Net 4.7.2 ou posterior.
- Você deve ter instalado o PowerShell 7.4.2 ou posterior.
- Você deve ter ativado o enfileiramento de mensagens do Windows.

- Você deve ser um administrador local no host.

Passos

1. Baixe o plug-in do SnapCenter para Microsoft Windows a partir do local de instalação.

   Por exemplo, o caminho de instalação padrão é C:/ProgramData/NetApp/SnapCenter/Repositório de pacotes.

   Este caminho é acessível a partir do host onde o servidor SnapCenter 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 variáveis por 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 são sensíveis a maiúsculas e minúsculas.

   Insira os valores para as seguintes variáveis:

Variável	Valor
/debuglog"<Debug_Log_Path>	Especifique o nome e o local do arquivo de log do instalador do pacote, como no exemplo a seguir: setup.exe /debuglog"C:
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.
BI_SERVICEACCOUNT	Especifique o plug-in do SnapCenter para a conta de serviço da Web do Microsoft Windows.

Variável	Valor
BI_SERVICEPWD	Especifique a senha do plug-in do SnapCenter para a conta do serviço da Web do Microsoft Windows.
ISFeatureInstall	Especifique a solução a ser implantada pelo SnapCenter em host remoto.

O parâmetro *debuglog* inclui o caminho do arquivo de log para o SnapCenter. Gravar neste arquivo de log é o método preferido de obter informações de solução de problemas, porque o arquivo contém os resultados das verificações que a instalação executa para pré-requisitos do plug-in.

Se necessário, você pode encontrar informações adicionais de solução de problemas no arquivo de log do pacote SnapCenter para Windows. Os arquivos de log para o pacote são listados (mais antigos primeiro) na pasta *%Temp%*, por exemplo, _C:

A instalação do plug-in para Windows Registra o plug-in no host e não no servidor SnapCenter. Você pode Registrar o plug-in no servidor SnapCenter adicionando o host usando a GUI do SnapCenter ou cmdlet do PowerShell. Depois que o host é adicionado, o plug-in é descoberto automaticamente.

Monitore o status da instalação do pacote de plug-in SnapCenter

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
   a. Clique em **filtro**.
   b. Opcional: Especifique a data de início e fim.
   c. No menu suspenso tipo, selecione **Instalação 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 **Visualizar logs**.

Configure o certificado CA

Gerar arquivo CSR do 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 a CSR gerada. O certificado terá uma chave privada associada a ele.

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

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

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

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

Para configurações de cluster, o nome do cluster (FQDN de cluster virtual) e os respetivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome alternativo (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados CA

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 **Yes**, importe a chave privada e clique em **Next**.
Importar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

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

7. Repita o passo 5 para a pasta "Pessoal".

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia 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 **thumbprint**.
   d. Copie os carateres 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

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.

Configure o certificado CA com os serviços de plug-in do host do Windows

Você deve configurar o certificado CA com os serviços de plug-in host do Windows para ativar o certificado digital instalado.

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, 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"
   ```

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet RUN *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando as *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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.

3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- * * Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da 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 são concluídas com êxito.

Instale o plug-in do SnapCenter para VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs) ou se você quiser proteger VMs e datastores, você deverá implantar o plug-in do SnapCenter para o dispositivo virtual VMware vSphere.

Para obter informações sobre como implantar, "Visão geral da implantação" consulte .

Implantar certificado CA

Para configurar o certificado CA com o plug-in SnapCenter para VMware vSphere, "Criar ou importar certificado SSL" consulte .

Configure o arquivo CRL

O plug-in do SnapCenter para VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL para o plug-in do SnapCenter para 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.

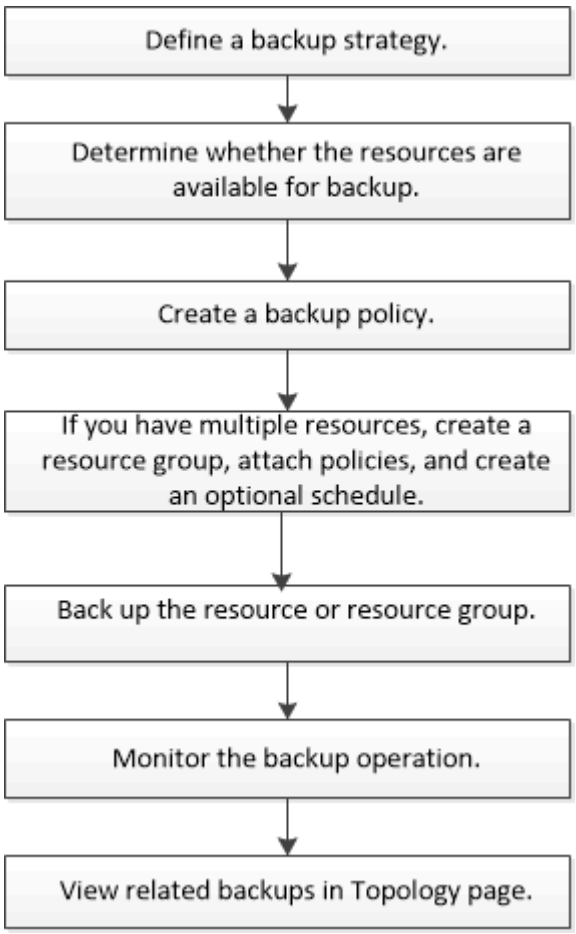
Faça backup dos sistemas de arquivos do Windows

Faça backup dos sistemas de arquivos do Windows

Ao instalar o plug-in do SnapCenter para Microsoft Windows em seu ambiente, você pode usar o SnapCenter para fazer backup de sistemas de arquivos do Windows. Você pode fazer backup de um único sistema de arquivos ou de um grupo de recursos que contenha 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 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 clone. A ajuda do cmdlet SnapCenter ou "Guia de referência de cmdlet do software SnapCenter" contém informações detalhadas sobre cmdlets do PowerShell.

Determinar a disponibilidade de recursos para sistemas de arquivos do Windows

Os recursos são os LUNs e componentes semelhantes no sistema de arquivos que são mantidos pelos plug-ins instalados. Você pode adicionar esses recursos a grupos de recursos para que você possa executar tarefas de proteção de dados em vários recursos, mas primeiro você deve identificar quais recursos você tem disponíveis. A descoberta de 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 servidor SnapCenter, adicionar hosts, criar conexões de máquina virtual de storage (SVM) e adicionar credenciais.
- Se os arquivos residirem em LUNs ou VMDKs do VMware RDM, você deverá implantar o plug-in do SnapCenter para VMware vSphere e Registrar o plug-in no SnapCenter. Para obter mais informações, "Plug-in do SnapCenter para documentação do VMware vSphere"consulte .

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 servidor SnapCenter.

   Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

Criar 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 criar uma nova política de backup no momento em que você cria um grupo de recursos ou quando faz backup de um recurso.

Antes de começar

- Você precisa ter definido sua estratégia de backup. "Saiba mais"
- Você precisa se preparar 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 storage (SVM).

- Se você estiver replicando snapshots em um storage secundário de espelhamento ou 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 false

- Reveja os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror. Para obter informações, "Limites de objetos para sincronização ativa do SnapMirror" consulte .

Sobre esta tarefa

- O SCRIPT_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 usar o caminho padrão para segurança.

  O valor da chave pode ser exibido do swagger através 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 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.

- Especificar um período de bloqueio instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na política.
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

As configurações do SnapLock primário são gerenciadas na política de backup do SnapCenter e as configurações do SnapLock secundário são gerenciadas pelo ONTAP.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **políticas**.
3. Para determinar se você pode usar uma política existente, selecione o nome da política e clique em **Detalhes**.

   Depois de analisar as políticas existentes, você pode executar um dos seguintes procedimentos:

   - Use uma política existente.
   - Copie uma política existente e modifique a configuração da política.
   - Crie uma nova política.
4. Para criar uma nova política, clique em **novo**.
5. Na página Nome, insira o nome da política e uma descrição.
6. Na página Opções de backup, execute as seguintes tarefas:

   a. Selecione uma definição de cópia de segurança.

Opção	Descrição
Backup consistente com o sistema de arquivos	Escolha esta opção se quiser que o SnapCenter silencie 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 no sistema de arquivos	Escolha esta opção se você não quiser que o SnapCenter silencie 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 têm agendas de backup diferentes.

   Se você tiver agendado para as 2:00 da manhã, o horário não será acionado durante o horário de verão (DST).

7. Na página retenção, especifique as configurações de retenção para backups sob demanda e para cada frequência de programação selecionada.

Opção	Descrição
Total de cópias Snapshot a reter	Escolha esta opção se quiser especificar o número de armazenamentos Snapshots SnapCenter antes de excluí-los automaticamente.
Excluir cópias Snapshot anteriores a	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 cópias snapshot	Selecione período de bloqueio instantâneo e selecione dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

Você deve definir a contagem de retenção para 2 ou superior. O valor mínimo para a contagem de retenção é 2.

O valor máximo de retenção é 1018 para recursos no ONTAP 9.4 ou posterior e 254 para recursos no ONTAP 9.3 ou anterior. Os backups falharão se a retenção for definida para um valor maior do que o que a versão subjacente do ONTAP suporta.

8. Na página replicação, especifique a replicação para o sistema de storage secundário:

Para este campo…	Faça isso…
Atualizar SnapMirror depois de criar uma cópia Snapshot local	Selecione esta opção para criar cópias espelhadas de conjuntos de backup em outro volume (SnapMirror). Essa opção deve estar habilitada para a 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. "Veja backups e clones relacionados na página topologia"Consulte .

Para este campo…	Faça isso…
Atualize o SnapVault depois de criar uma cópia 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 apenas no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão Atualizar na página topologia atualiza o período de bloqueio no secundário que é recuperado do ONTAP. Para obter mais informações sobre o SnapLock Vault, consulte "Armazene cópias Snapshot em WORM em um destino de cofre"
Etiqueta de política secundária	Selecione uma etiqueta Snapshot. Dependendo do rótulo de captura instantânea selecionado, o ONTAP aplica a política de retenção de snapshot secundária que corresponde ao rótulo. Se você selecionou **Atualizar SnapMirror depois de criar uma cópia Snapshot local**, você pode especificar opcionalmente o rótulo de política secundária. No entanto, se você selecionou **Atualizar SnapVault depois de criar uma cópia Snapshot local**, especifique o rótulo de política secundária.
Contagem de tentativas de erro	Insira o número de tentativas de replicação que devem ocorrer antes que o processo pare.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o storage secundário para evitar atingir o limite máximo de snapshots no storage secundário.

9. Na página Script, insira o caminho do prescritor ou postscript que você deseja que o servidor SnapCenter seja executado antes ou depois da operação de backup, respetivamente, e um limite de tempo que o SnapCenter espera que o script seja executado antes do tempo limite.

   Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas e enviar logs.

O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

10. Revise o resumo e clique em **Finish**.

Criar grupos de recursos para sistemas de arquivos do Windows

Um grupo de recursos é o contentor 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 tarefa de proteção de dados que deseja executar e, em seguida, especificar o agendamento de backup.

Sobre esta tarefa

- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.
- A adição de novos sistemas de arquivos sem a sincronização ativa do SnapMirror a um grupo de recursos existente que contenha recursos com a sincronização ativa do SnapMirror não é suportada.
- A adição de novos sistemas de arquivos a um grupo de recursos existente no modo failover da sincronização ativa do SnapMirror não é suportada. Você pode adicionar recursos ao grupo de recursos apenas no estado regular ou de failback.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **sistemas de arquivos** na lista.

Se você recentemente adicionou um sistema de arquivos ao SnapCenter, clique em **Atualizar recursos** para exibir 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	Introduza o nome do grupo de recursos. O nome do grupo de recursos não deve exceder 250 carateres.
Use o formato de nome personalizado para cópia Snapshot	Opcional: Insira um nome e formato personalizados do instantâneo. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

Para este campo…	Faça isso…
Etiqueta	Insira uma tag descritiva para ajudar ao 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 tiver adicionado recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois de atualizar sua lista de recursos.

   b. Na seção recursos disponíveis, clique nos sistemas de arquivos que você deseja fazer backup e, em seguida, clique na seta para a direita para movê-los para a seção adicionada.

      Se você selecionar a opção **Autoselect todos os recursos no mesmo volume de armazenamento**, todos os recursos no mesmo volume serão selecionados. Quando você os move para a seção adicionada, todos os recursos nesse volume se movem juntos.

   Para adicionar um único sistema de arquivos, desmarque a opção **seleção automática de todos os recursos no mesmo volume de armazenamento** e selecione os sistemas de arquivos que deseja mover para a seção adicionada.

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 você pode usar essa política.

      Se nenhuma política existente cumprir os seus requisitos, pode criar uma nova política clicando em para iniciar o assistente de política.

      As políticas selecionadas são listadas na coluna Política na seção Configurar programações para políticas selecionadas.

   b. Na seção Configurar agendas para políticas selecionadas, clique em na coluna Configurar agendas para a política para a qual você deseja configurar o agendamento.

   c. Se a política estiver associada a vários tipos de programação (frequências), selecione a frequência que pretende configurar.

   d. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação especificando a data de início, data de expiração e frequência e clique em **Finish**.

      As programações configuradas são listadas na coluna agendas aplicadas na seção Configurar programações para políticas selecionadas.

   As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas de backup do SnapCenter. Você não deve modificar as programações 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 por e-mail	Selecione **Always**, **on failure** ou **on failure or warning**, para enviar e-mails aos destinatários após criar grupos de recursos de backup, anexar políticas e configurar agendas. Introduza o servidor SMTP, a linha de assunto de e-mail padrão e os endereços de e-mail de e-mail de e para.
De	Endereço de e-mail
Para	E-mail para endereço
Assunto	Linha de assunto do e-mail padrão

8. Revise o resumo e clique em **Finish**.

   Você pode executar um backup sob demanda ou esperar que o backup agendado ocorra.

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 Administrador da infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estão em andamento.

  As instalações de plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento, pois 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 do sistema de armazenamento devem ser exclusivos.

  O SnapCenter não é compatível com vários sistemas de storage com o mesmo nome em clusters diferentes. Cada sistema de storage com suporte do SnapCenter deve ter um nome exclusivo e um endereço IP de 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Faça 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 uma relação SnapMirror com o armazenamento secundário, a função atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, 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 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 de arquivos de banco de dados. Isso cria um backup inconsistente e uma possível perda de dados ao restaurar. 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).

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 que 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 criando grupos de recursos.

4. Opcional: Na página recurso do assistente, insira um formato de nome personalizado para a captura Instantânea.

   Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

5. Na página políticas, execute as seguintes tarefas:

   a. Selecione uma ou mais políticas na lista suspensa.

      Você pode selecionar qualquer política existente e, em seguida, clique em **Detalhes** para determinar se você 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 para iniciar o assistente de política.

      As políticas selecionadas são listadas na coluna Política na seção Configurar programações para políticas selecionadas.

   b. Na seção Configurar agendas para políticas selecionadas, clique na coluna Configurar agendas para a política para a qual você deseja configurar o agendamento.

   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação especificando a data de início, data de expiração e frequência e clique em **Finish**.

      As programações configuradas são listadas na coluna agendas aplicadas na seção Configurar programações para políticas selecionadas.

   "As operações agendadas podem falhar"

6. Na página notificação, execute as seguintes tarefas:

Para este campo…	Faça isso…
Preferência por e-mail	Selecione **Always**, ou **On Failure**, ou **on failure ou Warning**, para enviar e-mails aos destinatários após criar grupos de recursos de backup, anexar políticas e configurar agendas. Insira as informações do servidor SMTP, a linha de assunto do e-mail padrão e os endereços de e-mail "'to'" e "'from'".
De	Endereço de e-mail
Para	E-mail para endereço
Assunto	Linha de assunto do e-mail padrão

7. Revise o resumo e clique em **Finish**.

   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 tiver aplicado 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. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

   É apresentado o aviso de nome de utilizador e palavra-passe.

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 CrashConsistent:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Descubra os recursos do host usando o cmdlet Get-SmResources.

   Este exemplo descobre os recursos do 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. Exiba o status da tarefa de backup usando o cmdlet Get-SmBackupReport.

   Este exemplo exibe um relatório de resumo de todos os trabalhos 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*. Em alternativa, pode também consultar o "Guia de referência de 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 uma programação configurada, os backups ocorrerão automaticamente de acordo com a programação.

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 uma relação SnapMirror com o armazenamento secundário, a função atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, 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 pode ser desencadeada tarde devido a problemas de rede. Você deve configurar o valor de MaxRetryForUninitializedHosts no web.config usando o cmdlet Set-SmConfigSettings PowerShell

Ao fazer backup de um sistema de arquivos, o SnapCenter não faz backup de LUNs 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 de arquivos de banco de dados. Isso cria um backup inconsistente e uma possível perda de dados ao restaurar. 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 **Resources** 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 e selecionando a tag. Em seguida, pode clicar para fechar o painel de filtro.

3. Na página grupos de recursos, selecione o grupo de recursos que deseja fazer backup e clique em **fazer backup agora**.

> Para o plug-in SnapCenter para banco de dados Oracle, se você tiver um grupo de recursos federados com dois bancos de dados e um do banco de dados 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 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. Clique em **Backup**.
5. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.
   - Nas configurações do MetroCluster, o SnapCenter pode não ser capaz de detetar uma relação de proteção após um failover.

     "Não é possível detetar a relação SnapMirror ou SnapVault após o failover do MetroCluster"

   - Se você estiver fazendo backup de dados de aplicativos em VMDKs e o tamanho de heap Java para o plug-in SnapCenter para VMware vSphere não for grande o suficiente, o backup pode falhar. Para aumentar o tamanho de heap Java, localize o arquivo de `/opt/netapp/init_scripts/scvservice` script . Nesse script, o `do_start method` 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. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado correspondente das operações:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera

- 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 a que apenas as operações de cópia de segurança sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Backup**.
   d. Na lista suspensa **Status**, selecione o status da cópia de segurança.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.

   Embora o status do trabalho de backup seja exibido , quando você clica nos detalhes do trabalho, você pode ver que algumas das tarefas secundárias da operação de backup ainda estão em andamento ou marcadas com sinais de aviso.

5. Na página Detalhes da tarefa, clique em **Exibir logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Monitorar operações no painel atividade

O painel atividade exibe as cinco operações mais recentes executadas. O painel atividade também é exibido quando a operação foi iniciada e o status da operação.

O painel atividade exibe informações sobre operações de backup, restauração, clone e backup agendadas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 da tarefa**.

Cancelar operações de cópia de segurança

Você pode cancelar as operações de backup que estão na fila.

O que você vai precisar

- Você deve estar logado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de cópia de segurança em execução.
- Você pode usar os comandos GUI, cmdlets do SnapCenter ou CLI para cancelar as operações de backup.

- O botão **Cancelar trabalho** está desativado 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 em fila de outros membros enquanto usa essa função.

Passos

1. Execute uma das seguintes ações:

A partir 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 da atividade	a. Depois de iniciar a operação de backup, clique em no painel atividade para exibir as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

A operação é cancelada e o recurso é revertido para o estado anterior.

Veja backups e clones relacionados na página topologia

Ao se preparar para fazer backup ou clonar um recurso, você poderá ver uma representação gráfica de todos os backups e clones no storage primário e secundário. Na página topologia, você pode ver todos os backups e clones disponíveis para o grupo de recursos ou recursos selecionado. Você pode visualizar os detalhes desses backups e clones e, em seguida, selecioná-los para executar operações de proteção de dados.

Sobre esta tarefa

Você pode revisar os ícones a seguir na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no storage primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups e clones disponíveis no storage primário.
- Exibe o número de backups e clones espelhados no storage secundário usando a tecnologia SnapMirror.

  Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

- Exibe o número de backups e clones replicados no storage secundário usando a tecnologia SnapVault.
  - O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou backups 6 usando uma política para reter apenas 4 backups, o número de backups exibidos será 6.
  - Se você atualizou do SnapCenter 1,1, os clones no secundário (espelho ou cofre) não serão exibidos em cópias espelhadas ou cópias do cofre na página topologia. Todos os clones criados usando o SnapCenter 1,1 são exibidos nas cópias locais no SnapCenter 3,0.

Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

Se você tiver uma relação secundária como sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), você poderá ver os seguintes ícones adicionais:

- O site da réplica está em cima.
- O site da réplica está inativo.
- A relação do espelho secundário ou do cofre não foi restabelecida.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o recurso ou o 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 de resumo para ver um resumo do número de backups e clones disponíveis no storage primário e secundário.

   A seção cartão de resumo exibe o número total de backups e clones. Somente para banco de dados Oracle, a seção cartão de resumo também exibe o número total de backups de log.

   Clicar no botão **Refresh** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clique no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Um horário semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo é espalhado por vários volumes, o tempo de expiração do SnapLock para o backup será o tempo de expiração do SnapLock mais longo definido para um snapshot em um volume. O tempo de expiração mais longo do SnapLock é recuperado do ONTAP.

   Para a 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 a relação de sincronização ativa do SnapMirror.

- Para a sincronização ativa do SnapMirror e somente para o ONTAP 9.14,1, as relações de espelhamento do Async ou EspelrorVault do Async com o novo destino primário devem ser configuradas manualmente após o failover. A partir do ONTAP 9.15,1 em diante, o espelho do Async ou o MirrorVault do Async 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 **Refresh** somente depois que um backup tiver sido criado.

5. No modo de 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 um 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 estão no sistema de armazenamento secundário.

7. Se você quiser excluir um clone, selecione o clone da tabela e clique para excluir o clone.

Exemplo mostrando backups e clones no armazenamento primário

Limpe a contagem de backup secundária usando cmdlets do PowerShell

Você pode usar o cmdlet Remove-SmBackup para limpar a contagem de backup para backups secundários que não têm Snapshot. Talvez você queira usar esse cmdlet quando o Total de snapshots exibido na topologia Gerenciar cópias não corresponder à configuração de retenção do Snapshot de storage 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 backup para backups secundários sem snapshots:

```
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"):
```

Restaure sistemas de arquivos do Windows

Restaure 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

- Tem de ter feito uma cópia de segurança do sistema de ficheiros.
- Se uma operação agendada, como uma operação de backup, estiver em andamento para um sistema de arquivos, essa operação deve 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.

  Você não pode 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 a partir de um backup do sistema de arquivos, você precisa clonar o backup e acessar o arquivo no clone.

- Não é possível restaurar um sistema ou um volume de inicialização.
- O SnapCenter pode restaurar sistemas de arquivos em um cluster do Windows sem deixar o grupo de cluster off-line.

Sobre esta tarefa

- O SCRIPT_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 usar o caminho padrão para segurança.

  O valor da chave pode ser exibido do swagger através 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 no local principal.
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 a partir de sistemas de storage primário ou secundário e, em seguida, selecione um backup para restaurar.
5. Selecione as opções no assistente Restaurar.
6. Você pode inserir o caminho e os argumentos do prescritor ou postscript que deseja que o SnapCenter execute antes ou depois da operação de restauração, respetivamente.

   Por exemplo, você pode executar um script para atualizar traps SNMP, automatizar alertas, enviar logs e assim por diante.

   O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

7. Na página notificação, selecione uma das seguintes opções:

Para este campo…	Faça isso…
Registre eventos do servidor SnapCenter no syslog do sistema de storage	Selecione esta opção para registar eventos do servidor SnapCenter no syslog do sistema de armazenamento.
Enviar notificação AutoSupport para operações com falha ao sistema de storage	Selecione esta opção para enviar informações sobre quaisquer operações com falha ao NetApp usando o AutoSupport.
Preferência por e-mail	Selecione **Always**, **on failure** ou **on failure or warning** para enviar mensagens de e-mail aos destinatários após restaurar os backups. Introduza o servidor SMTP, a linha de assunto de e-mail predefinida e os endereços de e-mail de e para.

8. Revise o resumo e clique em **Finish**.
9. Monitorize o progresso da operação clicando em **Monitor** > **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, o banco de dados pode 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 servidor SnapCenter 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 29th 2015 de janeiro a 3rd 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 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Restaure recursos usando cmdlets do PowerShell

A restauração de um backup de recurso inclui iniciar uma sessão de conexão com o servidor SnapCenter, listar os backups e recuperar informações de backup e 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 servidor SnapCenter 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 29th 2015 de janeiro a 3rd 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 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Monitorar as operações de restauração

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um 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 executar.

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso

- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Restore**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Cancelar operações de restauração

Você pode cancelar trabalhos de restauração que estão na fila.

Você deve estar logado como administrador do SnapCenter ou proprietário da tarefa para cancelar as operações de restauração.

Sobre esta tarefa

- Você pode cancelar uma operação de restauração em fila na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de restauração em execução.
- Você pode usar a GUI do SnapCenter, cmdlets do PowerShell ou os comandos CLI para cancelar as operações de restauração em fila.
- O botão **Cancelar trabalho** está desativado para operações de restauração que não podem ser canceladas.
- Se você selecionou **todos os membros desta função podem ver e operar em outros objetos membros** na página usuários/grupos ao criar uma função, você pode cancelar as operações de restauração em fila de outros membros enquanto usa essa função.

Passo

Execute uma das seguintes ações:

A partir 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 da atividade	1. Depois de iniciar a operação de restauração, clique no painel atividade para exibir as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

Clonar sistemas de arquivos do Windows

Clone 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, então você pode clonar um backup e acessar esse arquivo no clone.

Antes de começar

- Você deve se preparar para a proteção de dados concluindo tarefas como adicionar hosts, identificar recursos e criar conexões de máquina virtual de storage (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 storage (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 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 que você especificar.
- 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 para o agregado.
- Não é possível agendar operações de clone recorrente (ciclo de vida do clone) para sistemas de arquivos do Windows; só é possível clonar um backup sob demanda.
- Se você mover um LUN que contém um clone para um novo volume, o SnapCenter não poderá mais dar suporte ao 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 SCRIPT_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 usar o caminho padrão para segurança.

  O valor da chave pode ser exibido do swagger através 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 versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **sistemas de arquivos** na lista.
3. Selecione o host.

   A visualização de topologia é automaticamente exibida se o recurso estiver protegido.

4. Na lista recursos, selecione o backup que deseja clonar e clique no ícone clone.
5. Na página Opções, faça o seguinte:

Para este campo…	Faça isso…
Servidor clone	Escolha o host no qual o clone deve ser criado.
"'Auto Assign mount point'" ou "'Auto Assign volume mount point under path'"	Escolha se deseja atribuir automaticamente um ponto de montagem ou um ponto de montagem de volume sob um caminho. Atribuir automaticamente ponto de montagem de volume sob caminho: O ponto de montagem sob um caminho permite fornecer um diretório específico no qual os pontos de montagem serão criados. Antes de escolher essa opção, você deve verificar se o diretório está vazio. Se houver uma cópia de segurança no diretório, a cópia de segurança estará num estado inválido após a operação de montagem.
Localização do arquivo	Escolha um local de arquivamento se você estiver clonando um backup secundário.

6. Na página Script, especifique quaisquer prescripts ou postscripts que você deseja executar.

   O caminho de prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.

7. Revise o resumo e clique em **Finish**.
8. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 clone a partir de um backup existente usando o cmdlet New-SmClone.

   Este exemplo cria um clone a partir 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. Exiba o status da tarefa clone usando o cmdlet Get-SmCloneReport.

   Este exemplo exibe um relatório de clone para a ID de tarefa especificada:

```
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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Monitorar operações de clone

Você pode monitorar o andamento das operações de clone do SnapCenter usando a página tarefas. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera

- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista para que apenas operações de clone sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Cancelar operações de clone

Você pode cancelar as operações de clone que estão na fila.

Você deve estar logado como administrador do SnapCenter ou proprietário da tarefa para cancelar operações de clone.

Sobre esta tarefa

- Você pode cancelar uma operação de clone na fila a partir da página **Monitor** ou do painel **atividade**.
- Não é possível cancelar uma operação de clone em execução.
- Você pode usar a GUI do SnapCenter, cmdlets do PowerShell ou os comandos CLI para cancelar as operações de clone na fila.
- Se você selecionou **todos os membros desta função podem ver e operar em outros objetos membros** na página usuários/grupos enquanto cria uma função, você pode cancelar as operações de clone em fila de outros membros enquanto usa essa função.

Passo

Execute uma das seguintes ações:

A partir do…	Ação
Página do monitor	1. No painel de navegação esquerdo, clique em **Monitor** > **trabalhos**. 2. Selecione a operação e clique em **Cancelar trabalho**.

A partir do…	Ação
Painel da atividade	1. Depois de iniciar a operação clone, clique no painel atividade para exibir as cinco operações mais recentes. 2. Selecione a operação. 3. Na página **Detalhes do trabalho**, clique em **Cancelar trabalho**.

Divida um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido torna-se independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clones em um clone intermediário.

  Por exemplo, depois de criar clone1 a partir de um backup de banco de dados, você pode criar um backup de clone1 e clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e não é possível executar a operação de divisão de clones no clone1. No entanto, você pode executar a operação de divisão de clones no clone2.

  Depois de dividir clone2, você pode executar a operação de divisão de clones no clone1 porque clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e as tarefas de clone do clone são excluídas.
- Para obter informações sobre limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .
- Certifique-se de que o volume ou o agregado no sistema de storage esteja on-line.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página **recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicativos 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 do recurso é exibida.

4. No modo de 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 deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.

6. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

   A operação de divisão de clones deixa de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clones e tentar novamente a operação de divisão de clones.

   Se você quiser um tempo de enquete mais longo 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 que o SMCore busque o status da operação de divisão de clones. O valor é em milissegundos e o valor padrão é de 5 minutos.

   Por exemplo:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   A operação de inicialização dividida de clone falhará se o backup, a restauração ou outra divisão de clones estiver em andamento. Você deve reiniciar a operação de divisão de clones somente depois que as operações em execução estiverem concluídas.

Informações relacionadas

"O clone ou a verificação do SnapCenter falha com o agregado não existe"

Proteja os bancos de dados do Microsoft Exchange Server

Plug-in do SnapCenter para conceitos do Microsoft Exchange Server

Visão geral do plug-in do SnapCenter para Microsoft Exchange Server

O plug-in SnapCenter para Microsoft Exchange Server é um componente do lado do host do software NetApp SnapCenter que permite o gerenciamento de proteção de dados com reconhecimento de aplicativos de bancos de dados do Exchange. O plug-in para Exchange automatiza o backup e a restauração de bancos de dados do Exchange em seu ambiente SnapCenter.

Quando o plug-in para Exchange é instalado, você pode usar a tecnologia SnapCenter com NetApp SnapMirror para criar cópias espelhadas de conjuntos de backup em outro volume e com a tecnologia NetApp SnapVault para executar replicação de backup disco a disco para fins de conformidade ou arquivamento de padrões.

Se você quiser restaurar e recuperar e-mails ou caixa de correio em vez do banco de dados completo do Exchange, você pode usar o software Single Mailbox Recovery (SMBR). A recuperação de caixa de correio única NetApp chegou ao fim da disponibilidade (EOA) em 12 de maio de 2023. A NetApp continuará a oferecer suporte a clientes que adquiriram capacidade, manutenção e suporte da caixa de correio por meio de números de peça de marketing introduzidos em 24 de junho de 2020, durante o período do direito ao suporte.

O NetApp Single Mailbox Recovery é um produto parceiro fornecido pela Ontrack. O Ontrack PowerControls oferece recursos semelhantes aos da recuperação de caixa de correio única do NetApp. Os clientes podem adquirir novas licenças de software Ontrack PowerControls e renovações de manutenção e suporte Ontrack PowerControls do Ontrack (até licensingteam@ontrack.com) para recuperação granular da caixa de correio.

O plug-in para Exchange oferece suporte à sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), que permite que os serviços empresariais continuem operando mesmo com uma falha completa do local, dando suporte ao failover transparente de aplicativos usando uma cópia secundária. Nem a intervenção manual nem o script adicional são necessários para acionar um failover com a sincronização ativa do SnapMirror.

Ele dá suporte ao modo assimétrico, failover ou não duplex do SnapMirror ative Sync. Isso se refere à solução em que o caminho otimizado é apenas do nó proprietário do LUN do lado primário. Qualquer e/S vinda nos caminhos do cluster secundário é servida por proxy para o cluster primário. A replicação síncrona é unidirecional, na direção do primário para o secundário.

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 do Exchange (DAGs), bancos de dados e conjuntos de réplicas
- Defina políticas que fornecem 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 do Exchange primário e secundário
- Restaure bancos de dados de backups primários e secundários

Tipos de armazenamento suportados pelo plug-in SnapCenter para Microsoft Windows e para Microsoft Exchange Server

O SnapCenter suporta uma ampla variedade de tipos de armazenamento em máquinas físicas e máquinas virtuais. Você deve verificar se há suporte disponível para o seu tipo de armazenamento antes de instalar o pacote para o seu host.

O suporte para provisionamento e proteção de dados do SnapCenter está disponível no Windows Server. Para obter as informações mais recentes sobre versões suportadas, consulte a https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT [ferramenta de Matriz de interoperabilidade NetApp].

Máquina	Tipo de armazenamento	Provisione usando	Notas de suporte
Servidor físico	LUNs conectados a FC	Cmdlets da interface gráfica do usuário (GUI) do SnapCenter ou do PowerShell	
Servidor físico	LUNs ligados ao iSCSI	Cmdlets SnapCenter GUI ou PowerShell	
VMware VM	LUNs RDM ligados por um FC ou iSCSI HBA	Cmdlets do PowerShell	Apenas compatibilidade física VMDKs não são suportados.
VMware VM	ISCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets SnapCenter GUI ou PowerShell	VMDKs não são suportados.

Máquina	Tipo de armazenamento	Provisione usando	Notas de suporte
VM Hyper-V	LUNs de FC virtual (VFC) conectados por um switch Fibre Channel virtual	Cmdlets SnapCenter GUI ou PowerShell	Você deve usar o Hyper-V Manager para provisionar LUNs Virtual FC (VFC) conectados por um switch Fibre Channel virtual. O Hyper-V passa por discos e faz backup de bancos de dados em VHD(x) que são provisionados no armazenamento NetApp não são suportados.
VM Hyper-V	ISCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI	Cmdlets SnapCenter GUI ou PowerShell	O Hyper-V passa por discos e faz backup de bancos de dados em VHD(x) que são provisionados no armazenamento NetApp não são suportados.

ONTAP Privileges mínimo necessário para o plug-in do Exchange

Os ONTAP Privileges mínimos necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
  - event generate-AutoSupport-log
  - mostra o histórico de trabalhos
  - paragem do trabalho

- lun
- lun criar
- lun criar
- lun criar
- eliminação lun
- lun igrop add
- lun igrop criar
- eliminação do agrupamento lun
- mudar o nome do grupo lun
- mudar o nome do grupo lun
- show de grupos de lun
- nós complementares de mapeamento de lun
- mapeamento lun criar
- eliminação do mapeamento lun
- mapeamento lun remove-reporting-nonos
- mostra de mapeamento lun
- modificação de lun
- movimentação de lun no volume
- lun offline
- lun online
- limpeza da reserva persistente de lun
- redimensionar lun
- série lun
- mostra lun
- regra adicional de política do SnapMirror
- regra de modificação de política do SnapMirror
- regra de remoção da política do SnapMirror
- SnapMirror policy show
- restauração de SnapMirror
- SnapMirror show
- SnapMirror show-history
- atualização do SnapMirror
- SnapMirror update-ls-set
- SnapMirror lista-destinos
- versão
- clone de volume criar
- show de clone de volume

- início da divisão do clone de volume
- paragem dividida clone volume
- criar volume
- destruição de volume
- clone de arquivo de volume criar
- show-disk-use do arquivo de volume
- volume off-line
- volume online
- modificação do volume
- criar qtree de volume
- eliminação de qtree de volume
- modificação de qtree de volume
- apresentação de qtree de volume
- restrição de volume
- apresentação do volume
- criar instantâneo de volume
- eliminar instantâneo do volume
- modificação do instantâneo do volume
- tempo de expiração do volume snapshot modify-SnapLock
- mudar o nome do instantâneo do volume
- restauração de snapshot de volume
- restauração de arquivo de snapshot de volume
- apresentação de instantâneo do volume
- desmontar o volume
- svm cifs
- compartilhamento cifs de svm criar
- exclusão de compartilhamento cifs de svm
- apresentação do shadowcopy cifs de svm
- exibição de compartilhamento cifs de svm
- mostra cifs de svm
- política de exportação de svm
- criação de política de exportação de svm
- exclusão da política de exportação do svm
- regra de política de exportação de svm criar
- a regra de política de exportação do svm é exibida
- exibição da política de exportação do svm
- svm iscsi

- apresentação da ligação iscsi de svm
- mostra o svm

- Comandos somente leitura: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
  - interface de rede
  - mostra da interface de rede
  - svm

Preparar sistemas de storage para replicação SnapMirror e SnapVault

Você pode usar um plug-in do 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 disco a disco para conformidade com os padrões e outros fins relacionados à governança. Antes de executar essas tarefas, você deve configurar uma relação de proteção de dados entre os volumes de origem e destino e inicializar a relação.

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 . Se você estiver usando a sincronização ativa do SnapMirror , use os agendamentos padrão do SnapMirror ou SnapVault para a sincronização ativa do SnapMirror e para relacionamentos assíncronos.

Se você estiver vindo para o SnapCenter de um produto NetApp SnapManager e estiver satisfeito com as relações de proteção de dados que configurou, ignore esta seção.

Uma relação de proteção de dados replica dados no storage primário (o volume de origem) para o storage secundário (o volume de destino). Ao inicializar a relação, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não suporta relações em cascata entre volumes SnapMirror e SnapVault (**Primary** > **Mirror** > **Vault**). Você deve usar relacionamentos de fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis de versão e como configurá-los, consulte "Documentação do ONTAP".

Defina uma estratégia de backup para recursos do Exchange Server

Definir uma estratégia de backup antes de criar seus trabalhos de backup ajuda a garantir que você tenha os backups necessários para restaurar seus bancos de dados com êxito. Seu Contrato de nível de serviço (SLA), objetivo de tempo de recuperação (rto) e objetivo do ponto de restauração (RPO) determinam em grande parte a sua estratégia de backup.

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados 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 era dos arquivos que precisam ser recuperados do storage de backup para que as operações regulares sejam retomadas após uma falha. O SLA, rto e RPO contribuem para a estratégia de backup.

Tipos de backups suportados para o banco de dados Exchange

Fazer backup de caixas de correio do Exchange usando o SnapCenter requer que você escolha o tipo de recurso, como bancos de dados e grupos de disponibilidade de banco de dados (DAG). A tecnologia Snapshot é utilizada para criar cópias on-line e somente leitura dos volumes nos quais os recursos residem.

Tipo de cópia de segurança	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 transação que já estão comprometidos com o banco de dados. Normalmente, você deve escolher essa 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 transação truncados não são backup.
Registo de cópia de segurança	Faz backup de todos os logs de transação. Os logs truncados que já estão comprometidos com o banco de dados não são copiados. Se você agendar backups frequentes de log de transações entre backups completos de bancos de dados, poderá escolher pontos de recuperação granular.

Agendas de backup para plug-ins de banco de dados

A frequência de backup (tipo de agendamento) é especificada em políticas; uma programação de backup é especificada na configuração do grupo de recursos. O fator mais crítico na determinação de uma 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 usado a cada hora, enquanto você pode fazer backup de um recurso raramente usado uma vez por dia. Outros fatores incluem a importância do recurso para a sua organização, seu Contrato de nível de Serviço (SLA) e seu objetivo de ponto de recuperação (RPO).

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. Um RPO define a estratégia para a era dos arquivos que precisam ser recuperados do storage 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 usado, não é necessário executar um backup completo mais de uma ou duas vezes por dia. Por exemplo, backups regulares de log de transações podem ser suficientes para garantir que você tenha os backups necessários. Quanto mais você fizer backup de seus bancos de dados, menos Registros de transações que o SnapCenter precisa usar no momento da restauração, o que pode resultar em operações de restauração mais rápidas.

Os programas de backup têm duas partes, como segue:

- Frequência de backup

  A frequência de backup (com que frequência os backups devem ser executados), chamada *schedule type* para alguns plug-ins, faz parte de uma configuração de política. Você pode selecionar a frequência de backup da política por hora, dia, semanal ou mensal. Se você não selecionar nenhuma dessas frequências, a política criada será uma política somente sob demanda. Você pode acessar políticas clicando em **Configurações** > **políticas**.

- Fazer backup de programações

  As agendas 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 que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas. Você pode acessar programações de 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 de que você precisa 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 padrão de nomenclatura Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um carimbo de data/hora aos nomes de Snapshot 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 carimbo de data/hora.

Como alternativa, você pode especificar o formato do nome da captura Instantânea enquanto protege recursos ou grupos de recursos selecionando **usar formato de nome personalizado para cópia Instantânea**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do carimbo de hora é adicionado ao nome do instantâneo.

Opções de retenção de backup

Você pode escolher o número de dias para os quais reter cópias de backup ou especificar o número de cópias de backup que deseja reter, até um máximo de ONTAP de 255 cópias. Por exemplo, sua organização pode exigir que você retenha 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 tiver sido alterado para o grupo de recursos ou recursos, os backups com o rótulo de tipo de agendamento antigo ainda poderão permanecer no sistema.

Para retenção de longo prazo de cópias de backup, você deve usar o backup SnapVault.

Quanto tempo para reter backups de log de transações no volume de armazenamento de origem para o Exchange Server

O plug-in do 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 tempo entre dois backups completos.

Por exemplo, se o Plug-in para Exchange fez um backup completo do log de transações mais às 8:00 da manhã e outro backup completo do log de transações mais às 5:00 da tarde, ele poderia usar o backup de log de transações mais recente para restaurar o banco de dados a qualquer momento entre as 8:00 da manhã e as 5:00 da tarde se os logs de transações não estiverem disponíveis, o Plug-in para Exchange pode executar apenas operações de restauração pontual, que restaura

Normalmente, você precisa de operações de restauração mais atualizadas por apenas um dia ou dois. Por padrão, o SnapCenter mantém um mínimo de dois dias.

Defina uma estratégia de restauração para bancos de dados do Exchange

Definir uma estratégia de restauração para o Exchange Server permite restaurar 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.

É possível restaurar bancos de dados somente do storage primário.

Tipos de operações de restauração compatíveis com o Exchange Server

Você pode usar o SnapCenter para executar diferentes tipos de operações de restauração em recursos do Exchange.

- Restaurar mais atualizado
- Restaurar para um ponto anterior no tempo

Restaure até o minuto

Em uma operação de restauração atualizada, os bancos de dados são recuperados até o ponto de falha. O SnapCenter realiza 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 transação que foram copiados, bem como quaisquer novos logs que foram criados desde o backup mais recente.

   Os logs de transações são movidos para frente e aplicados a quaisquer bancos de dados selecionados.

   O Exchange cria uma nova cadeia de log após a conclusão de uma restauração.

   Prática recomendada: recomenda-se 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.

   Depois de executar uma restauração atualizada, o backup usado para a restauração estará disponível apenas 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 de log de transações do sistema por meio das políticas de backup.

Restaurar para um ponto anterior no tempo

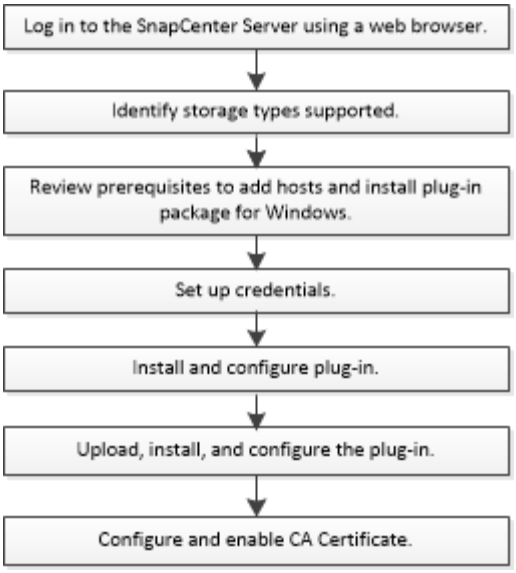
Em uma operação de restauração pontual, os bancos de dados são restaurados apenas para um tempo específico do passado. Uma operação de restauração pontual ocorre nas seguintes situações de restauração:

- O banco de dados é restaurado para um determinado tempo em um log de transação de backup.
- O banco de dados é restaurado e apenas um subconjunto de logs de transações de backup é aplicado a ele.

Instale o plug-in do SnapCenter para o Microsoft Exchange Server

Fluxo de trabalho de instalação do plug-in SnapCenter para Microsoft Exchange Server

Você deve instalar e configurar o plug-in do SnapCenter para o Microsoft Exchange Server se quiser proteger bancos de dados do Exchange.



Pré-requisitos para adicionar hosts e instalar o plug-in do SnapCenter para Microsoft Exchange Server

Antes de adicionar um host e instalar os pacotes de plug-in, você deve completar todos os requisitos.

- Se estiver a utilizar iSCSI, o serviço iSCSI tem de estar em execução.
- Você deve ter um usuário de domínio com Privileges de administrador local com permissões de login local no host remoto.
- Você deve estar usando o Microsoft Exchange Server 2013, 2016 ou 2019 para configurações autônomas e do grupo de disponibilidade de banco de dados.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host.
- Se você gerenciar nós de cluster no SnapCenter, precisará ter um usuário com Privileges administrativo 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 deve cancelar o Registro do provedor de hardware VSS 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 for Microsoft Exchange Server e o Plug-in for Exchange estiverem instalados no mesmo servidor, você deverá suspender ou excluir do agendador do Windows todas as programações criadas pelo SnapManager para o Microsoft Exchange Server.
- O host deve ser resolvido para o nome de domínio totalmente qualificado (FQDN) do servidor. Se o arquivo hosts for modificado para torná-lo resoluvel e se o nome curto e o FQDN forem especificados no arquivo hosts, crie uma entrada no arquivo SnapCenter hosts no seguinte formato: *<ip_address> <host_fqdn> <host_name>*.
- Certifique-se de que as seguintes portas não estão bloqueadas no firewall, caso contrário, a operação de adição de host falha. Para resolver esse problema, você deve configurar o intervalo de portas dinâmicas. Para obter mais informações, "Documentação da Microsoft"consulte .

- 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 dínyicport tcp
- netsh int ipv4 show dynamicport udp
- netsh int ipv6 mostra dínyicport tcp
- netsh int ipv6 show dynamicport udp

Requisitos de host para instalar o pacote de plug-ins do 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 do sistema host e requisitos de dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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	• .NET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet."

É necessário o Exchange Server Privileges

Para permitir que o SnapCenter adicione o Exchange Server ou DAG e instale o plug-in do SnapCenter para o Microsoft Exchange Server em um host ou DAG, você deve configurar o SnapCenter com credenciais para um usuário com um conjunto mínimo de Privileges e permissões.

Você deve ter um usuário de domínio com o administrador local Privileges 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:

- Add-MailboxDatabaseCopy
- Desmontar a base de dados
- Get-AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Get-MailboxStatistics
- Get-PublicFolderDatabase
- Mover-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly: True
- Monte-base de dados
- New-MailboxDatabase
- New-PublicFolderDatabase
- Remover-MailboxDatabase
- Remove-MailboxDatabaseCopy
- Remover-PublicFolderDatabase

- Resume-MailboxDatabaseCopy
- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore: Verdadeiro
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy
- Update-MailboxDatabaseCopy

Requisitos de host para instalar o pacote de plug-ins do 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 do sistema host e requisitos de dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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	• .NET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade 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-ins 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 do Windows. Embora você possa criar credenciais para o Windows depois de implantar hosts e instalar plug-ins, a prática recomendada é criar credenciais após adicionar SVMs, antes de implantar hosts e instalar plug-ins.

Configure as credenciais com o administrador Privileges, incluindo direitos de administrador no host remoto.

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

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Clique em **novo**.

   É apresentada a janela Credential (credencial).

4. Na página Credential (credencial), faça o seguinte:

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para a credencial.

Para este campo…	Faça isso…
Nome de utilizador	Introduza o nome de utilizador utilizado 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 no qual você está instalando o plug-in do SnapCenter. Formatos válidos para o campo Nome de usuário são: ◦ `NetBIOS\UserName` ◦ `Domain FQDN\UserName` • Administrador local (apenas para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é: `UserName`
Palavra-passe	Introduza a palavra-passe utilizada para autenticação.
Autenticação	Selecione Windows como o modo de autenticação.

5. Clique em **OK**.

Configure o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite criar uma conta de serviço gerenciado de grupo (gMSA) que fornece gerenciamento automatizado de senha de conta de serviço a partir de uma conta de domínio gerenciado.

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 é um membro do domínio.

Passos

1. Crie uma chave raiz KDS para gerar senhas exclusivas para cada objeto em seu gMSA.
2. Para cada domínio, execute o seguinte comando do 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,…>
.. Execute `Get-ADServiceAccount` o comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Ative o módulo do ative Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando do 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 o host.

b. Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua o Privileges administrativo ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no servidor SnapCenter.

   O servidor SnapCenter 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.

Adicione hosts e instale o Plug-in para o 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 para um cluster.

Antes de começar

- Se o sistema operacional do host do servidor SnapCenter for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deve executar o seguinte:
  - Atualize para o Windows Server 2019 (versão de SO 17763,5936) ou posterior
  - Atualize para o Windows Server 2022 (versão de SO 20348,2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como o administrador do SnapCenter
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host.
- O serviço de enfileiramento de mensagens deve estar em execução.
- Se você estiver usando a conta de serviço gerenciado de grupo (gMSA), você deve configurar o gMSA com Privileges administrativo. Para obter informações, "Configure a conta de serviço gerenciado de grupo no Windows Server 2016 ou posterior para o Microsoft Exchange Server"consulte .

Sobre esta tarefa

- Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.
- 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 servidor SnapCenter.
- Se você estiver instalando plug-ins em um cluster (Exchange DAG), eles serão instalados em todos os nós do cluster, mesmo que alguns dos nós não tenham bancos de dados em LUNs NetApp.

A partir do SnapCenter 4,6, o SCE é compatível com a alocação a vários clientes e você pode adicionar um host usando os seguintes métodos:

Adicionar operação de host	4,5 e anteriores	4,6 e mais tarde
Adicione DAG sem IP em domínio cruzado ou diferente	Não suportado	Suportado

Adicionar operação de host	4,5 e anteriores	4,6 e mais tarde
Adicione vários DAGs IP com nomes exclusivos, residindo no mesmo domínio ou entre domínios	Suportado	Suportado
Adicione vários DAGs IP ou sem IP que tenham os mesmos nomes de host e/ou nome de banco de dados no domínio cruzado	Não suportado	Suportado
Adicione vários DAGs sem IP/IP com o mesmo nome e domínio cruzado	Não suportado	Suportado
Adicione 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, você deve cancelar o Registro do provedor de hardware VSS usado pelo SnapDrive para Windows porque é incompatível com o provedor de hardware VSS instalado com o pacote plug-in para Exchange e plug-ins do SnapCenter para Windows. Para obter mais informações, "Como Registrar manualmente o Fornecedor de hardware VSS do Data ONTAP"consulte .

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Verifique se **hosts gerenciados** está selecionado na parte superior.
3. Clique em **Add**.
4. Na página hosts, faça o seguinte:

Para este campo…	Faça isso…
Tipo de host	Selecione **Windows** como o tipo de host. O servidor SnapCenter adiciona o host e, em seguida, instala no host o plug-in para Windows e o plug-in para Exchange se eles ainda não estiverem 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 foi instalada anteriormente, o SnapCenter atualiza a versão como parte da instalação.

Para este campo…	Faça isso…
Nome do host	Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada 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 fizer parte de um subdomínio, você deverá fornecer o FQDN. Você pode inserir endereços IP ou o FQDN de uma das seguintes opções: • Anfitrião independente • Trocar DAG Para um DAG do Exchange, 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 IP less DAG fornecendo o endereço IP ou o FQDN de um dos nós do cluster DAG. ◦ Adicione IP menos DAG que resida no mesmo domínio ou domínio diferente. Você também pode adicionar vários DAGs IP/IP menos com o mesmo nome, mas domínios diferentes. Para um host autônomo ou um DAG do Exchange (entre domínios ou mesmo domínio), é recomendável fornecer FQDN ou o endereço IP do host ou do DAG.

Para este campo…	Faça isso…
Credenciais	Selecione o nome da credencial que você criou ou crie as novas credenciais. A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte informações sobre como criar uma credencial. Você pode exibir 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 instalar.

   Quando você seleciona Plug-in para Exchange, o plug-in do 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 a outro uso de recursos exigido pelo Exchange.

6. (Opcional) clique em **mais opções**.

Para este campo…	Faça isso…
Porta	Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido 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, você deve especificar a mesma porta. Caso contrário, a operação falha.
Caminho de instalação	O caminho padrão é `C:\Program Files\NetApp\SnapCenter`. Opcionalmente, você pode personalizar o caminho.
Adicione todos os hosts no DAG	Marque essa caixa de seleção quando adicionar um DAG.

Para este campo…	Faça isso…
Ignorar as verificações de pré-instalação	Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	Marque essa caixa de seleção se quiser usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in. Forneça o nome gMSA no seguinte formato: _Domainname O gMSA será usado como uma conta de serviço de logon apenas para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

   Se você não tiver selecionado 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 poderá atualizar o arquivo web.config localizado no `C:\Program Files\NetApp\SnapCenter` WebApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, será necessário atualizar o arquivo em ambos os nós.

8. Monitorize o progresso da instalação.

Configure a porta personalizada para comunicação NET TCP

Por padrão, começando com a versão do SnapCenter 6,0, o plug-in do SnapCenter para Windows usa a porta 909 para comunicação DE REDE TCP. Se a porta 909 estiver em uso, você poderá configurar outra porta para comunicação TCP de REDE.

Passos

1. Modifique o valor da chave *NetTCPPort* localizada em _C:/Program Files/NetApp/SnapCenter/SnapCenter Plug-in para o número de porta necessário.
   `<add key="NetTCPPort" value="new_port_number" />`
2. Modifique o valor da chave *NetTCPPort* localizada em _C:/arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in para o número de porta necessário.
   `<add key="NetTCPPort" value="new_port_number" />`
3. Desmarque o 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 é 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 está agora exibido na lista de serviços em *services.msc*.

5. Reinicie o serviço *Plug-in para Windows*.

Instale o plug-in para o Exchange a partir do host do servidor SnapCenter usando cmdlets do PowerShell

Você deve instalar o plug-in para Exchange a partir da GUI do SnapCenter. Se você não quiser usar a GUI, você pode usar cmdlets do PowerShell no host do servidor SnapCenter ou em um host remoto.

Antes de começar

- O servidor SnapCenter deve ter sido instalado e configurado.
- Você deve ser um administrador local no host ou um usuário com Privileges administrativo.
- Você deve ser um usuário atribuído a uma função que tenha permissões de plug-in, instalação e desinstalação, como o Admin do SnapCenter
- 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 que o plug-in para Exchange seja instalado deve ser um host do Windows.

Passos

1. No host do servidor SnapCenter, 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*. Em alternativa, pode também consultar o "Guia de referência de 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 com o SnapCenter.

Instale o plug-in SnapCenter para Exchange silenciosamente a partir da linha de comando

Você deve instalar o plug-in para o Exchange a partir da interface de usuário do SnapCenter. No entanto, se você não puder por algum motivo, você pode executar o programa de instalação Plug-in para Exchange sem supervisão no modo silencioso a partir da linha de comando do Windows.

Antes de começar

- Você deve ter feito backup de seus recursos do Microsoft Exchange Server.
- Você deve ter instalado os pacotes plug-in do SnapCenter.
- Você deve excluir a versão anterior do plug-in do SnapCenter para Microsoft SQL Server antes de instalar.

  Para obter mais informações, "Como instalar um plug-in do SnapCenter manualmente e diretamente do host do plug-in"consulte .

Passos

1. Valide se a pasta *C: /Temp* existe no host do plug-in e o usuário conetado tem acesso total a ela.
2. Faça o download do plug-in do SnapCenter para o Microsoft Windows a partir do repositório *C:/ProgramData/NetApp/SnapCenter/Package*.

   Este caminho é acessível a partir do host onde o servidor SnapCenter 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 para o qual 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"<Debug_Log_Path>" /log"<Log_Path>" BI_SnapCenter_PORT<Num> SUITE_INSTALLDIR"<Install_Directory_Path>" BI_SERVICEACCOUNT <domain\administrator> BI_SERVICEPWD_<password>

   Por exemplo:

   NetApp: SnapCenter_Windows_host_plugin.exe"/silent /debuglog"C: HPPW_SCSQL_Install.log" /log"C: Temp" BI_SnapCenter_PORT_8145 SUITE_INSTALLDIR"C: SnapCenter NetApp_SnapCenter

   Todos os parâmetros passados durante a instalação do Plug-in para Exchange são sensíveis a maiúsculas e minúsculas.

   Insira os seguintes valores para as variáveis:

Variável	Valor
/debuglog"<Debug_Log_Path>	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.
BI_SERVICEACCOUNT	Especifique o plug-in do SnapCenter para a conta de serviço da Web do Microsoft Windows.

Variável	Valor
BI_SERVICEPWD	Especifique a senha do plug-in do SnapCenter para a conta do serviço da Web do Microsoft Windows.
ISFeatureInstall	Especifique a solução a ser implantada pelo SnapCenter em 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 para Exchange Registra o plug-in no host e não no servidor SnapCenter. Você pode Registrar o plug-in no servidor SnapCenter adicionando o host usando a GUI do SnapCenter ou cmdlet do PowerShell. Depois que o host é adicionado, o plug-in é descoberto automaticamente.

Monitore o status da instalação do pacote de plug-in SnapCenter

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
   a. Clique em **filtro**.
   b. Opcional: Especifique a data de início e fim.
   c. No menu suspenso tipo, selecione **Instalação 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 **Visualizar logs**.

Configurar certificado CA

Gerar arquivo CSR do 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 a CSR gerada. O certificado terá uma chave privada associada a ele.

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

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

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

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

Para configurações de cluster, o nome do cluster (FQDN de cluster virtual) e os respetivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome alternativo (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados CA

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 **Yes**, importe a chave privada e clique em **Next**.
Importar formato de ficheiro	Não faça alterações; clique em **seguinte**.

Nesta janela do assistente…	Faça o seguinte…
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

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

7. Repita o passo 5 para a pasta "Pessoal".

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia 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 **thumbprint**.
   d. Copie os carateres 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

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.

Configure o certificado CA com os serviços de plug-in do host do Windows

Você deve configurar o certificado CA com os serviços de plug-in host do Windows para ativar o certificado digital instalado.

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, 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"
```

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet RUN *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando as *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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- * * Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da 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 são concluídas com êxito.

Configure o SnapManager 7.x para Exchange e SnapCenter para coexistir

Para ativar o plug-in do SnapCenter para Microsoft Exchange Server para coexistir com o SnapManager para Microsoft Exchange Server, é necessário instalar o plug-in do SnapCenter para Microsoft Exchange Server no mesmo servidor Exchange no qual o SnapManager para Microsoft Exchange está instalado, desativar as programações do SnapManager para Exchange e configurar novas programações e backups usando o plug-in do SnapCenter 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 que você não precisa mais.
- Você deve ter suspenso ou excluído todas as agendas criadas pelo SnapManager para Microsoft Exchange Server do agendador do Windows.
- O plug-in do SnapCenter para Microsoft Exchange Server e o SnapManager para Microsoft Exchange Server podem coexistir no mesmo Exchange Server, mas não é possível atualizar as instalações existentes do SnapManager para o SnapCenter.

  O SnapCenter não fornece uma opção para a atualização.

- O SnapCenter não suporta a restauração de bancos de dados do Exchange a partir do backup do SnapManager para o Microsoft Exchange Server.

  Se você não desinstalar o SnapManager para Microsoft Exchange Server após a instalação do plug-in do SnapCenter para Microsoft Exchange Server e depois desejar restaurar um backup do SnapManager para Microsoft Exchange Server, você deve executar etapas adicionais.

Passos

1. Usando o PowerShell em todos os nós DAG, determine se o provedor de hardware SnapDrive para Windows VSS 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, desmarque o provedor de hardware VSS do SnapDrive para Windows: *navssprv.exe -r Service –u*
3. Verifique se o provedor de hardware VSS foi removido: *Vssadmin list providers*
4. Adicione o host do Exchange ao SnapCenter e, em seguida, instale o plug-in do SnapCenter para Microsoft Windows e o plug-in do SnapCenter para Microsoft Exchange Server.
5. No diretório do plug-in do SnapCenter para Microsoft Windows em todos os nós DAG, verifique se o provedor de hardware do VSS está registrado: *Vsadmin 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. Pare as programações de backup do SnapManager para Microsoft Exchange Server.
7. Usando a GUI do SnapCenter, crie backups sob demanda, configure backups programados e configure configurações de retenção.
8. Desinstale o SnapManager para o Microsoft Exchange Server.

   Se você não desinstalar o SnapManager para Microsoft Exchange Server agora e depois deseja restaurar um backup do SnapManager para Microsoft Exchange Server:

   a. Desmarque o plug-in do SnapCenter 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. A partir do 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*

Instale o plug-in do SnapCenter para VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs) ou se você quiser proteger VMs e datastores, você deverá implantar o plug-in do SnapCenter para o dispositivo virtual VMware vSphere.

Para obter informações sobre como implantar, "Visão geral da implantação" consulte .

Implantar certificado CA

Para configurar o certificado CA com o plug-in SnapCenter para VMware vSphere, "Criar ou importar certificado SSL" consulte .

Configure o arquivo CRL

O plug-in do SnapCenter para VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL para o plug-in do SnapCenter para 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.

Preparar-se para a proteção de dados

Antes de executar qualquer operação de proteção de dados, como operações de backup, clone ou restauração, você precisa definir sua estratégia e configurar o ambiente. Você também pode configurar o servidor SnapCenter para usar a tecnologia SnapMirror e SnapVault.

Para aproveitar as tecnologias SnapVault e SnapMirror, você deve configurar e inicializar uma relação 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

"Primeiros passos com a REST API"

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 servidor SnapCenter e executar as tarefas de pré-requisito.

- Instalar e configurar o servidor SnapCenter.
- Inicie sessão no SnapCenter.
- Configure o ambiente SnapCenter adicionando ou atribuindo conexões do sistema de storage e criando uma credencial.

> O SnapCenter não é compatível com vários SVMs com o mesmo nome em clusters diferentes. Cada SVM com suporte do SnapCenter precisa ter um nome exclusivo.

- Adicione hosts, instale o plug-in do SnapCenter para Microsoft Windows e o plug-in do SnapCenter para Microsoft Exchange Server e descubra (atualizar) os recursos.
- Execute o provisionamento de storage no lado do host usando o plug-in do SnapCenter para Microsoft Windows.
- Se você estiver usando o servidor SnapCenter para proteger bancos de dados do Exchange que residem nos LUNs VMware RDM, você deverá implantar o plug-in do SnapCenter para VMware vSphere e Registrar o plug-in no SnapCenter. A documentação do plug-in do SnapCenter para VMware vSphere tem mais informações.

  VMDKs não são suportados.

- Mova um banco de dados existente do Microsoft Exchange Server de um disco local para o armazenamento suportado usando as ferramentas do Microsoft Exchange.
- Configure as relações do SnapMirror e do SnapVault, se quiser fazer backup da replicação.

Para usuários do SnapCenter 4.1.1, a documentação do plug-in do SnapCenter para VMware vSphere 4.1.1 tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos. Para usuários do SnapCenter 4,2.x, o Agente de dados do NetApp 1,0 e 1,0.1, a documentação tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in do SnapCenter para 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 plug-in do SnapCenter para VMware vSphere 4,3 tem informações sobre como proteger bancos de dados virtualizados e sistemas de arquivos usando o plug-in SnapCenter baseado no Linux para o dispositivo virtual VMware vSphere (formato Open Virtual Appliance).

"Plug-in do SnapCenter para documentação do 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 semente 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 DAG (Grupo de disponibilidade de banco de dados do Microsoft Exchange) que 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.

  Quando você executa uma operação em um grupo de recursos, executa essa operação nos recursos definidos no grupo de recursos de acordo com a programação especificada para o grupo de recursos.

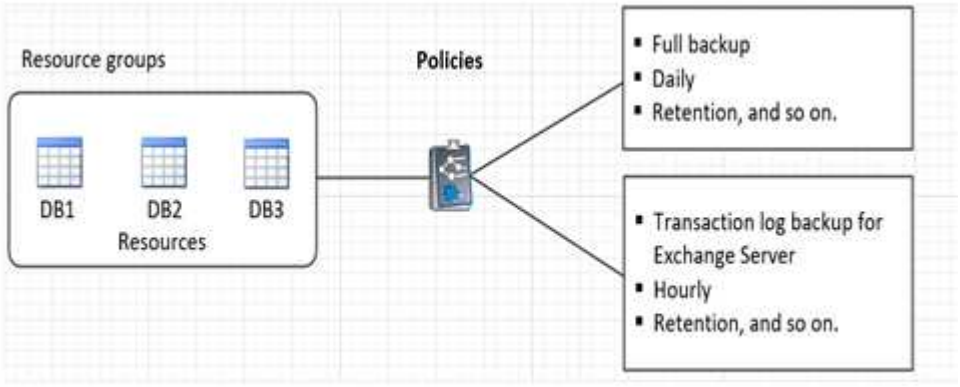
  Você pode fazer backup sob demanda de um único recurso ou de um grupo de recursos. Você também pode executar backups programados para recursos únicos e grupos de recursos.

  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 definindo *o que* você quer proteger e quando você quer protegê-lo em termos de dia e tempo. Pense em uma política como definindo *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. Em seguida, você pode anexar duas políticas ao grupo de recursos: Uma política diária e uma política por hora. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diário e outro agendamento que executa backups de log por hora. A imagem a seguir ilustra a relação entre recursos, grupos de recursos e políticas para bancos de dados:



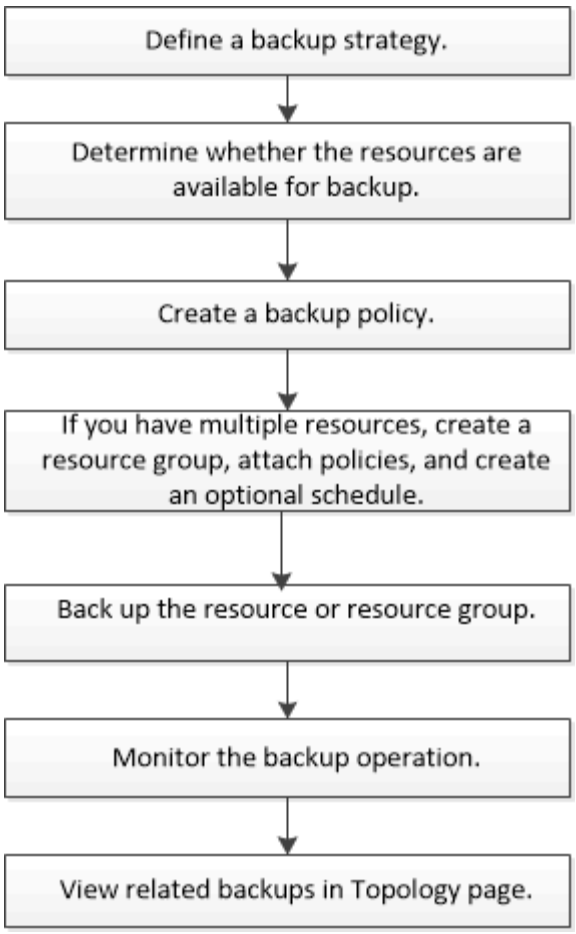
Faça backup dos recursos do Exchange

Fluxo de trabalho de backup

Ao instalar o plug-in do SnapCenter para Microsoft Exchange Server em seu ambiente, você pode usar o SnapCenter para fazer backup dos recursos do Exchange.

Você pode agendar vários backups para serem executados em 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:



Exchange banco de dados e verificação de backup

O plug-in do 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 servidor Exchange. O utilitário permite que você execute verificações de consistência para verificar a integridade dos bancos de dados e backups do Exchange.

Prática recomendada: não é necessário realizar verificações de consistência em bancos de dados que fazem parte de uma configuração do grupo de disponibilidade de banco de dados (DAG) com pelo menos duas réplicas.

Para obter informações adicionais, "Documentação do Microsoft Exchange Server"consulte .

Determine se os recursos do Exchange estão disponíveis para backup

Os recursos são os bancos de dados, os grupos de disponibilidade do banco de dados do Exchange que são mantidos pelos plug-ins instalados. Você pode adicionar esses recursos a grupos de recursos para que você possa executar tarefas de proteção de dados, mas primeiro você deve identificar quais recursos você tem disponíveis. A determinação dos recursos disponíveis também verifica se a instalação do plug-in foi

concluída com êxito.

Antes de começar

- Você já deve ter concluído tarefas como instalar o servidor SnapCenter, adicionar hosts, criar conexões do sistema de storage, adicionar credenciais e instalar o plug-in para o 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 VMware RDM, você deverá implantar o plug-in do SnapCenter para VMware vSphere e Registrar o plug-in no SnapCenter. O "Plug-in do SnapCenter para documentação do 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 **Estado geral** está definida como não disponível para cópia de segurança quando qualquer uma das seguintes situações for verdadeira:
  - Os bancos de dados não estão em um LUN NetApp.
  - Os bancos de dados não estão no estado normal.

    Os bancos de dados não estão no estado normal quando estão no estado de montagem, desmontagem, semente de novo 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 o trabalho de backup do DAG.

Passos

1. No painel de navegação esquerdo, clique em **recursos** e selecione **Microsoft Exchange Server** na lista suspensa 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 DAG 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. Em seguida, pode 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 servidor SnapCenter.

   > Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

   Os recursos são exibidos juntamente com informações como nome do recurso, nome do grupo de disponibilidade do banco de dados, servidor no qual o banco de dados está ativo atualmente, 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 armazenamento não NetApp e se pelo

menos uma cópia passiva do banco de dados estiver em armazenamento NetApp, não protegido será exibido na coluna **Estado geral**.

Não é possível executar operações de proteção de dados em um banco de dados que esteja em um tipo de storage que não seja NetApp.

- Se o banco de dados estiver em armazenamento NetApp e não estiver protegido, não protegido será exibido na coluna **Estado geral**.
- Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, a interface do usuário exibirá a mensagem Backup not run na coluna **Estado 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 successed na coluna **Estado 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 criar uma política de backup no momento em que criar um grupo de recursos ou fazer backup de um único recurso.

Antes de começar

- Você precisa 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 precisa se preparar para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, identificar recursos e criar conexões do sistema de storage.
- Você deve ter atualizado (descoberto) os recursos do Exchange Server.
- Se você estiver replicando snapshots em um espelhamento ou cofre, o administrador do SnapCenter deverá ter atribuído as máquinas virtuais de storage (SVMs) para os volumes de origem e de destino a você.
- Se você quiser executar os scripts do PowerShell em prescripts e postscripts, defina o valor do `usePowershellProcessforScripts` parâmetro como true no `web.config` arquivo.

  O valor padrão é false.

- Reveja os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror. Para obter informações, "Limites de objetos para sincronização ativa do SnapMirror" consulte .

Sobre esta tarefa

- Uma política de backup é um conjunto de regras que regem como você gerencia e retém backups e com que frequência o backup do recurso ou do grupo de recursos é feito. 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 total de backup é específica de uma determinada política. Um banco de dados ou recurso que usa a política A com uma retenção total de backup 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 aplica-se 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 SCRIPT_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 usar o caminho padrão para segurança.

  O valor da chave pode ser exibido do swagger através da API: API /4,7/configsettings

  Você pode usar a API GET para exibir o valor da chave. A API SET não é suportada.

  Prática recomendada: é melhor configurar a política de retenção secundária com base no número de backups completos e de log, no geral, que você deseja manter. Ao configurar políticas de retenção secundárias, lembre-se de que quando bancos de dados e logs que estão em volumes diferentes, cada backup pode ter três snapshots e, quando bancos de dados e logs estão no mesmo volume, cada backup pode ter dois snapshots.

- SnapLock
  - Se a opção 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.

    Especificar um período de bloqueio instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na política.

    Para as versões ONTAP 9.12,1 e inferiores, os clones criados a partir dos snapshots de cofre do SnapLock herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

    As configurações do SnapLock primário são gerenciadas na política de backup do SnapCenter e as configurações do SnapLock secundário 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 a descrição da política.
5. Na página tipo de backup, execute as seguintes etapas:
   a. Escolha o tipo de cópia de segurança:

Se você quiser…	Faça isso…
Faça backup dos arquivos do banco de dados e dos logs de transação necessários	Selecione **cópia de segurança completa e cópia de segurança de registo**. 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.
Faça backup dos arquivos do banco de dados e dos logs de transação não confirmados	Selecione **cópia de segurança completa**. Os bancos de dados são copiados com truncamento de log e os logs truncados não são copiados.
Faça backup de todos os logs de transação	Selecione **Log backup**. Todos os logs de transação no sistema de arquivos ativo são copiados e não há truncamento de log. Um diretório *scebackupinfo* é criado no mesmo disco do log ao vivo. Este diretório contém o ponteiro para as alterações incrementais para o 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 **cópia de segurança**. Todos os bancos de dados e todos os logs são copiados, e não há truncamento de log. Você normalmente usa esse tipo de backup para uma réplica de nova propagação ou para testar ou diagnosticar um problema.

Você deve definir o espaço necessário para backups de log com base na retenção completa do backup e não com base na retenção de até o minuto (UTM).

Crie políticas de Vault separadas para logs e bancos de dados ao lidar com LUNs (volumes do Exchange) e defina manter (retenção) para a política de log como o dobro do número de cada rótulo da política de banco de dados, usando os mesmos rótulos. Para obter mais informações, consulte, "Os backups do SnapCenter para Exchange mantêm apenas metade dos snapshots no volume de log de destino do Vault"

b. Na seção Configurações do grupo de disponibilidade de banco de dados, selecione uma ação:

Para este campo…	Faça isso…
Fazer backup de cópias ativas	Selecione esta opção para fazer backup apenas das cópias ativas do banco de dados selecionado. Para grupos de disponibilidade de banco de dados (DAGs), essa opção faz backup apenas de cópias ativas de todos os bancos de dados no DAG. Cópias passivas não são backup.
Faça backup de cópias 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, essa opção faz backup de cópias ativas e passivas de todos os bancos de dados nos servidores selecionados.

Nas 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 mudar, os backups do nó proprietário anterior serão mantidos. A retenção é aplicável apenas no nível do nó.

c. Na seção frequência de programação, selecione um ou mais tipos de frequência: **Sob demanda**, **hora**, **diária**, **semanal** e **mensal**.

Você pode especificar a programação (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 atribuir diferentes programações de backup a cada política.

Se você tiver agendado para as 2:00 da manhã, o horário não será acionado durante o horário de verão (DST).

6. Na página retenção, configure as definições de retenção.

As opções apresentadas dependem do tipo de cópia de segurança e do tipo de frequência que selecionou anteriormente.

O valor máximo de retenção é 1018 para recursos no ONTAP 9.4 ou posterior e 254 para recursos no ONTAP 9.3 ou anterior. Os backups falharão se a retenção for definida para um valor maior do que o que a versão subjacente do ONTAP suporta.

Você deve definir a contagem de retenção como 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro snapshot é o snapshot de referência para a relação 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…
Guarde 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 restaurações atualizadas. A retenção atualizada (UTM) aplica-se ao backup de log criado por meio de backup completo ou de log. Por exemplo, se as configurações de retenção 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 dos backups completos e de log são automaticamente excluídas como parte do UTM. Não é possível eliminar manualmente as pastas de registo. Por exemplo, se a configuração de retenção de backup completo ou completo e de log for definida para 1 mês e retenção UTM for definida para 10 dias, a pasta de log criada como parte desses backups será excluída conforme UTM. Como resultado, apenas 10 dias de pastas de log estarão lá e todos os outros backups serão marcados para restauração pontual. Você pode definir o valor de retenção UTM como 0, se não quiser executar a restauração mais atualizada. Isso permitirá a operação de restauração pontual. **Prática recomendada:** é melhor que a configuração seja igual à configuração de totais instantâneos (backups completos) na seção Configurações de retenção de backup completo. Isso garante que os arquivos de log sejam mantidos para cada backup completo.
Guarde as cópias de backup por um número específico de dias	Selecione a opção **manter backups de log para a última** 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 instantâneo	Selecione **período de bloqueio de cópias instantâneas** 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 mantidos como parte das configurações de retenção atualizadas para backups completos.

b. Na seção Configurações completas de retenção de backup, selecione uma das opções a seguir para backups sob demanda e, em seguida, selecione uma para backups completos:

Para este campo…	Faça isso…
Guarde apenas um número específico de instantâneos	Se você quiser especificar o número de backups completos a serem mantidos, selecione a opção **Total de cópias snapshot a serem mantidas** e especifique o número de snapshots (backups completos) a serem mantidos. Se o número de backups completos exceder o número especificado, os backups completos que excedem o número especificado serão excluídos, com as cópias mais antigas excluídas primeiro.
Guarde backups completos por um número específico de dias	Selecione a opção **manter cópias Snapshot para** e especifique o número de dias para manter as capturas instantâneas (backups completos).
Período de bloqueio instantâneo	Selecione **período de bloqueio de cópias instantâneas** e selecione dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

Se você tiver um banco de dados com somente 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 neste 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 somente backups de log adicionando a chave **MaxLogBackupOnlyCountWithoutFullBackup** no arquivo *C: Arquivos de programas/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 replicação, selecione uma ou ambas as seguintes opções de replicação secundária:

Para este campo…	Faça isso…
Atualize o SnapMirror depois de criar um instantâneo 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 estar ativada para a 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 ativar 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. "Veja backups do Exchange na página topologia"Consulte .
Atualize o SnapVault depois de criar um instantâneo local	Selecione esta opção para executar a replicação de backup de disco para disco.
Etiqueta de política secundária	Selecione uma etiqueta Snapshot. Dependendo do rótulo de captura instantânea selecionado, o ONTAP aplica a política de retenção de snapshot secundária que corresponde ao rótulo. Se você selecionou **Atualizar SnapMirror depois de criar uma cópia Snapshot local**, você pode especificar opcionalmente o rótulo de política secundária. No entanto, se você selecionou **Atualizar SnapVault depois de criar uma cópia Snapshot local**, especifique o rótulo de política secundária.

Para este campo…	Faça isso…
Contagem de tentativas de erro	Insira o número de tentativas de replicação que devem ocorrer antes que o processo pare.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o storage secundário para evitar atingir o limite máximo de snapshots no storage secundário.

8. Na página Script, insira o caminho e os argumentos do prescritor ou postscript que devem ser executados antes ou depois da operação de backup, respetivamente.
   - Os argumentos de backup do Prescript incluem ""base de dados"" e ""ServerInstance"".
   - Os argumentos de backup PostScript incluem ""base de dados"", ""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 prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_path.
9. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas para Exchange Servers

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 tarefa de proteção de dados que deseja executar e o cronograma de proteção.

Sobre esta tarefa

- O SCRIPT_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 usar o caminho padrão para segurança.

  O valor da chave pode ser exibido do swagger através 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 versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.
- A adição de novos bancos de dados sem a sincronização ativa do SnapMirror a um grupo de recursos existente que contenha recursos com a sincronização ativa do SnapMirror não é suportada.
- A adição de novos bancos de dados a um grupo de recursos existente no modo failover da sincronização ativa do SnapMirror não é suportada. Você pode adicionar recursos ao grupo de recursos apenas no estado regular ou de failback.

Passos

1. No painel de navegação à esquerda, 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 recentemente adicionou um recurso ao SnapCenter, clique em **Atualizar recursos** para exibir 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	Introduza o nome do grupo de recursos. O nome do grupo de recursos não deve exceder 250 carateres.
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.
Use o formato de nome personalizado para cópia Snapshot	Opcional: Insira um nome e formato personalizados do instantâneo. Por exemplo, *customtext_resourcegroup_policy_hostname* ou *resourcegroup_hostname*. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

5. Na página recursos, execute as seguintes etapas:
   a. Selecione o tipo de recurso e o Grupo de disponibilidade de banco de dados nas listas suspensas para filtrar a lista de recursos disponíveis.

      Se você tiver adicionado recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois de 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. Esse FQDN indica apenas que o banco de dados está ativo nesse host específico e pode não fazer backup nesse host. Você deve selecionar um ou mais servidores de backup na opção de seleção de servidor, onde você deseja fazer backup caso tenha selecionado a opção **Backup de cópias em servidores a serem selecionados no momento de criação da tarefa 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 **seleção automática de 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 instantâneo. Se houver mais de 30 bancos de dados em um grupo de recursos, um segundo Snapshot será criado para os bancos de dados adicionais. Por conseguinte, são criadas 2 subtarefas no trabalho de cópia de segurança principal. Para backups com replicação secundária, enquanto a atualização do SnapMirror ou do SnapVault estiver em andamento, pode haver cenários em que a atualização para ambos os subtrabalhos se sobreponham. O trabalho de backup principal continua em execução para sempre, mesmo se os logs indicarem que o trabalho está 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 **Backup de cópias em servidores a serem selecionados na hora de criação da tarefa de backup**, uma opção de seleção de servidor será exibida para selecionar um ou mais servidores. A opção de seleção de servidor irá listar apenas o servidor onde o banco de dados selecionado está no armazenamento NetApp.

      Na seção Configurar agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Na seção Configurar agendas para políticas selecionadas, clique em + na coluna **Configurar agendas** para a política para a qual você deseja configurar o agendamento.

   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação especificando a data de início, data de expiração e frequência e clique em **OK**.

      Você deve fazer isso para cada frequência listada na política. As programações configuradas são listadas na coluna **programações aplicadas** na seção Configurar programações para políticas selecionadas.

   As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas 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 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 o comando GUI ou 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

8. Revise o resumo e clique em **Finish**.

Crie uma conexão de sistema de armazenamento e uma credencial usando cmdlets do PowerShell para 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 restauração.

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 Administrador da infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estão em andamento.

  As instalações de plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento, pois 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 do sistema de armazenamento devem ser exclusivos.

  O SnapCenter não é compatível com vários sistemas de storage com o mesmo nome em clusters diferentes. Cada sistema de storage com suporte do SnapCenter deve ter um nome exclusivo e um endereço IP de 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 storage 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 Run as 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Faça backup de bancos de dados do Exchange

Se um banco de dados não fizer parte de qualquer 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 precisa 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 uma relação SnapMirror com um armazenamento secundário, a função atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.
- Se pretender efetuar uma cópia de segurança de uma base de dados ou de um grupo de disponibilidade de bases de dados ativo/passivo num armazenamento NetApp e não NetApp, e tiver selecionado **cópia de segurança de cópias ativas** ou **cópia de segurança de cópias de segurança em servidores a selecionar durante o tempo de criação da tarefa de cópia de segurança** na política, os trabalhos de cópia de segurança entrarão no estado de aviso. O backup será bem-sucedido para cópia de banco de dados ativo/passivo no armazenamento NetApp e o backup falhará para cópia de banco de dados ativo/passivo em armazenamento não NetApp.

Prática recomendada: 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.

IU do SnapCenter

Passos

1. No painel de navegação à esquerda, 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 ícone indica que o banco de dados está em armazenamento não NetApp.

   Em um DAG, se uma cópia de banco de dados ativo estiver em um armazenamento não NetApp e pelo menos uma cópia de banco de dados passivo residir em um armazenamento NetApp, você poderá proteger o banco de dados.

   Clique em e selecione o nome do host e o tipo de banco de dados para filtrar os recursos. Em seguida, pode clicar em * * para fechar o painel do filtro.

   - Se você quiser fazer backup de um banco de dados, clique no nome do banco de dados.
     i. Se a vista topologia for apresentada, clique em **Protect**.
     ii. Se for apresentado o assistente Database - Protect Resource (base de dados - proteger recurso), avance para o passo 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 instantâneo personalizado, na página recursos, marque a caixa de seleção **usar formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

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 **Backup de cópias em servidores a serem selecionados na hora de criação da tarefa 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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique em * * na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

   c. Na janela Adicionar programações para a política *policy_name*, configure a programação e clique

em **OK**.

Onde, *policy_name* é o nome da política selecionada.

As programações configuradas são listadas na coluna agendas aplicadas.

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 quiser anexar o relatório da operação de backup realizada no recurso, 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-SmtpServer.

6. Revise o resumo e clique em **Finish**.

   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 tiver aplicado 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 ser capaz de detetar uma relação de proteção após um failover.

     Para obter informações, consulte: "Não é possível detetar a relação SnapMirror ou SnapVault após o failover do MetroCluster"

   - Se você estiver fazendo backup de dados de aplicativos em VMDKs e o tamanho de heap Java para o plug-in SnapCenter para VMware vSphere não for grande o suficiente, o backup pode 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 servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-smconnection  -SMSbaseurl
https://snapctr.demo.netapp.com:8146/
```

É apresentado o aviso de nome de utilizador e palavra-passe.

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 tipo de backup do 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 tipo de backup do 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 apenas de logs do Exchange:

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

3. Descubra os recursos do host usando o cmdlet Get-SmResources.

   Este exemplo descobre os recursos do 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 DAG (Exchange Database Availability Group) 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 no storage secundário:

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

6. Exiba o status da tarefa de backup usando o cmdlet Get-SmBackupReport.

Este exemplo exibe um relatório de resumo de todos os trabalhos executados na data especificada:

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

Este exemplo apresenta um relatório de resumo de trabalhos para uma ID de trabalho específica:

```
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*. Em alternativa, "Guia de referência de cmdlet do software SnapCenter"consulte .

Faça backup dos 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 storage (SVM) usada pelo banco de dados.
- Se você quiser fazer backup de um recurso que tenha uma relação SnapMirror com um armazenamento secundário, a função atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, 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 pode começar tarde devido a problemas de rede. Você deve configurar o valor de `MaxRetryForUninitializedHosts` in `web.config` usando o `Set-SmConfigSettings` cmdlet PowerShell.
- Em um grupo de recursos, se você incluir um banco de dados ou um grupo de disponibilidade de banco de dados que tenha cópia de banco de dados ativo/passivo em um armazenamento NetApp e não NetApp e tiver selecionado **fazer backup de cópias ativas** ou **fazer backup de cópias em servidores a serem selecionadas durante o tempo de criação da tarefa de backup** na política, os trabalhos de backup entrarão no estado de aviso.

  O backup será bem-sucedido para cópia de banco de dados ativo/passivo no armazenamento NetApp e o backup falhará para cópia de banco de dados ativo/passivo em armazenamento 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 uma programação configurada, os backups ocorrerão automaticamente de acordo com a programação.

Passos

1. No painel de navegação à esquerda, 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. Em seguida, pode clicar em* * para fechar o painel do filtro.
3. Na página grupos de recursos, selecione o grupo de recursos que deseja fazer backup e clique em **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. 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. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado correspondente das operações:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- 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 a que apenas as operações de cópia de segurança sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Backup**.
   d. Na lista suspensa **Status**, selecione o status da cópia de segurança.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.

   Embora o status do trabalho de backup seja exibido , quando você clica nos detalhes do trabalho, você pode ver que algumas das tarefas secundárias da operação de backup ainda estão em andamento ou marcadas com sinais de aviso.

5. Na página Detalhes da tarefa, clique em **Exibir logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Monitorar operações no painel atividade

O painel atividade exibe as cinco operações mais recentes executadas. O painel atividade também é exibido

quando a operação foi iniciada e o status da operação.

O painel atividade exibe informações sobre operações de backup, restauração, clone e backup agendadas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 da tarefa**.

Cancelar operações de backup para o banco de dados do Exchange

Você pode cancelar as operações de backup que estão na fila.

O que você vai precisar

- Você deve estar logado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de cópia de segurança em execução.
- Você pode usar os comandos GUI, cmdlets do SnapCenter ou CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** está desativado 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 em fila de outros membros enquanto usa essa função.

Passos

1. Execute uma das seguintes ações:

A partir 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 da atividade	a. Depois de iniciar a operação de backup, clique em no painel atividade para exibir as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

A operação é cancelada e o recurso é revertido para o estado anterior.

Veja backups do Exchange na página topologia

Quando você estiver se preparando para fazer backup de um recurso, talvez seja útil exibir 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 grupo de recursos ou recursos selecionado. Você pode exibir 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 storage primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups disponíveis no armazenamento primário.
- Exibe o número de backups espelhados no storage secundário usando a tecnologia SnapMirror.
- Exibe o número de backups replicados no storage secundário usando a tecnologia SnapVault.
  - O número de backups exibidos inclui os backups excluídos do armazenamento secundário.

    Por exemplo, se você criou backups 6 usando uma política para reter apenas 4 backups, o número de backups exibidos é 6.

Prática recomendada: para garantir que o número correto de backups replicados seja exibido, recomendamos que você atualize a topologia.

Se você tiver uma relação secundária como sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), você poderá ver os seguintes ícones adicionais:

- O site da réplica está em cima.
- O site da réplica está inativo.
- A relação do espelho secundário ou do cofre não foi restabelecida.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 é exibida.

4. Consulte a seção cartão de 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 **Refresh** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clique no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Um horário semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo é espalhado por vários volumes, o tempo de expiração do SnapLock para o backup será o tempo de expiração do SnapLock mais longo definido para um snapshot em um volume. O tempo de expiração mais longo do SnapLock é recuperado do ONTAP.

   Para a 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 a relação de sincronização ativa do SnapMirror.

   - Para a sincronização ativa do SnapMirror e somente para o ONTAP 9.14,1, as relações de espelhamento do Async ou EspelrorVault do Async com o novo destino primário devem ser configuradas manualmente após o failover. A partir do ONTAP 9.15,1 em diante, o espelho do Async ou o MirrorVault do Async são configurados automaticamente para o novo destino principal.após o failover.
   - Após o failover, um backup deve ser criado para que o SnapCenter esteja ciente do failover. Você pode clicar em **Refresh** somente depois que um backup tiver sido criado.

5. No modo de exibição Gerenciar cópias, clique em **backups** no armazenamento primário ou secundário para ver detalhes de um backup.

   Os detalhes dos backups são exibidos em um 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.

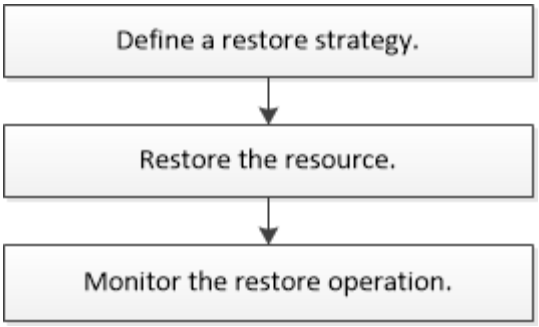
   Não é possível renomear ou excluir backups que estão no armazenamento secundário. A exclusão de snapshots é tratada pelas configurações de retenção do ONTAP.

Restaure os recursos do Exchange

Restaure o fluxo de trabalho

Você pode usar o SnapCenter para restaurar bancos de dados do Exchange restaurando um ou mais backups no seu sistema de arquivos ativo.

O fluxo de trabalho a seguir mostra a sequência na qual você deve executar as operações de restauração de 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 "Guia de referência de cmdlet do software SnapCenter" consulte .

Requisitos para restaurar um banco de dados do Exchange

Antes de restaurar um banco de dados do Exchange Server a partir de um plug-in do SnapCenter para backup do Microsoft Exchange Server, você deve garantir que vários requisitos sejam atendidos.

Para usar completamente a funcionalidade de restauração, você deve atualizar o servidor SnapCenter e o plug-in SnapCenter para o banco de dados Exchange para 4,6.

- O Exchange Server deve estar on-line e em execução antes de poder restaurar um banco de dados.
- Os bancos de dados devem existir no Exchange Server.

  Restaurar bancos de dados excluídos não é suportado.

- As programações do SnapCenter para o banco de dados devem ser suspensas.
- O servidor SnapCenter e o plug-in do SnapCenter para o host do Microsoft Exchange Server devem estar conetados ao storage primário e secundário que contém os backups que você deseja restaurar.

Restaure 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, banco de dados ou 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 em um espelho ou cofre, o administrador do SnapCenter deverá ter atribuído as SVMs para os volumes de origem e os volumes de destino.
- Em um DAG, se uma cópia de banco de dados ativo estiver em um armazenamento não NetApp e você quiser restaurar a partir do backup de cópia de banco de dados passivo que está em um armazenamento NetApp, faça 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 de volta no mesmo host e nenhum novo volume é criado.
- Os backups no nível DAG devem ser restaurados a partir de bancos de dados individuais.
- A restauração completa do disco não é suportada quando existem ficheiros diferentes do ficheiro de base 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 os usados para replicação. Quando uma restauração completa pode afetar a funcionalidade do Exchange, o Plug-in para Exchange executa uma única operação de restauração de arquivo.

- O plug-in para Exchange não pode restaurar unidades criptografadas BitLocker.
- O SCRIPT_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 usar o caminho padrão para segurança.

  O valor da chave pode ser exibido do swagger através 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 versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage 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 no local principal.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** no canto superior esquerdo da página recurso.
2. Selecione o plug-in do Exchange Server na lista suspensa.
3. Na página recursos, selecione **Banco de dados** na lista Exibir.
4. Selecione a base de dados na lista.
5. No modo de 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	Escolha **todos os backups de log** para executar a operação de restauração de backup atualizada para restaurar todos os backups de log disponíveis após o backup completo.
Por backup 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 no UTM. Por exemplo, se a retenção total do backup for 5 e a retenção UTM for 3, o número de backups de log disponíveis será 5, mas na lista suspensa somente 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 em que os logs de transação são aplicados ao banco de dados restaurado. Essa operação de restauração pontual restaura as entradas de log de transações que foram registradas até o último backup na data e hora especificadas.
Nenhum	Escolha **nenhum** quando precisar restaurar somente o backup completo sem nenhum backup de log.

Você pode executar uma das seguintes ações:

- * Recuperar e montar banco de dados após restauração * - esta opção é selecionada por padrão.
- **Não verifique a integridade dos logs de transação no backup antes da restauração** - por padrão, o SnapCenter verifica a integridade dos logs de transação em um backup antes de executar uma operação de restauração.

  Prática recomendada: você não deve selecionar essa opção.

7. Na página Script, insira o caminho e os argumentos do prescritor ou postscript que devem ser executados antes ou depois da operação de restauração, respetivamente.

   Os argumentos de restauração incluem Banco de dados e ServerInstance.

   Os argumentos de restauração postscript incluem banco de dados, 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 prescripts ou postscripts não deve incluir unidades ou compartilhamentos. O caminho deve ser relativo ao SCRIPT_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 **Finish**.
10. Você pode exibir o status do trabalho de restauração expandindo o painel atividade na parte inferior da página.

    Deve monitorizar o processo de restauro utilizando a página **Monitor** > **trabalhos**.

Quando você restaura um banco de dados ativo de um backup, o banco de dados passivo pode entrar no estado suspenso ou com falha se houver um atraso entre a réplica e o banco de dados ativo.

A alteração de estado pode ocorrer quando a cadeia de registo da base de dados ativa se bifurca e inicia uma nova ramificação que quebra a replicação. O Exchange Server tenta corrigir a réplica, mas se não conseguir fazê-lo, após a restauração, você deve criar um novo backup e, em seguida, semear novamente a réplica.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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. Restaure 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 pontual:

```
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 storage secundário para um story 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` parâmetro permite especificar os volumes primário e secundário que deseja usar para a restauração.

O `-IsRecoverMount:$true` parâmetro permite montar 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Recuperação granular de e-mails e caixa de correio

O software Single Mailbox Recovery (SMBR) permite restaurar e recuperar e-mails ou caixa de correio em vez do banco de dados completo do Exchange.

Restaurar banco de dados completo apenas para recuperar um único e-mail vai consumir muito tempo e recursos. O SMBR ajuda a recuperar rapidamente os e-mails criando uma cópia clone do Snapshot e, em seguida, usando as API da Microsoft para montar a caixa de correio no SMBR. Para obter informações sobre como usar o SMBR, "Guia de administração DE SMBR" consulte .

Para obter informações adicionais sobre SMBR, consulte o seguinte:

- "Como restaurar manualmente um único item com SMBR (também aplicável para restaurações de Controle de Energia Ontrack)"
- "Como restaurar do armazenamento secundário em SMBR com o SnapCenter"
- "Recuperando o Microsoft Exchange Mail do SnapVault usando SMBR"

Restaure um banco de dados do Exchange Server a partir do armazenamento secundário

Você pode restaurar um banco de dados do Exchange Server de backup do armazenamento secundário (espelho ou cofre).

Você precisa ter replicado os snapshots do storage primário para um storage secundário.

Sobre esta tarefa

- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage 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 no local principal.

Passos

1. No painel de navegação à esquerda, 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** no sistema de armazenamento secundário (espelho ou cofre).
5. Selecione a cópia de segurança 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 **Finish**.

Semente novamente uma réplica passiva do nó Exchange

Se você precisar semear novamente uma cópia de réplica, por exemplo, quando uma cópia está corrompida, você pode semear novamente para o backup mais recente usando o recurso Reseed no SnapCenter.

Antes de começar

- Você deve estar usando o servidor SnapCenter 4,1 ou posterior e o plug-in para o Exchange 4,1 ou posterior.

  Nova propagação uma réplica não é suportada em versões do SnapCenter anteriores a 4,1.

- Você deve ter criado um backup do banco de dados que deseja fazer o repleed.

Prática recomendada: para evitar o atraso entre nós, recomendamos que você crie um novo backup antes de executar uma operação de semente novamente ou escolha o host com o backup mais recente.

Passos

1. No painel de navegação à esquerda, 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 semente de novo um único banco de dados	Selecione **Banco de dados** na lista Exibir.
Para reseed bancos de dados em um DAG	Selecione **Grupo de disponibilidade da base de dados** na lista Ver.

3. Selecione o recurso que você deseja fazer a semente novamente.
4. Na página Gerenciar cópias, clique em **Reseed**.
5. Na lista de cópias de bancos de dados não saudáveis no assistente Reseed, selecione a que deseja reseed e, em seguida, clique em **Next**.
6. Na janela Host, selecione o host com o backup a partir do qual você deseja semente novamente e clique em **Next**.
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 **Finish**.
9. Você pode exibir o status do trabalho expandindo o painel atividade na parte inferior da página.

A operação Reseed não é suportada se a cópia passiva do banco de dados residir em armazenamento não NetApp.

Reseed uma réplica usando cmdlets do PowerShell para o banco de dados do Exchange

Você pode usar cmdlets do PowerShell para restaurar uma réplica não saudável 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o `Open-SmConnection` cmdlet.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Semente novamente o banco de dados usando o `reseed-SmDagReplicaCopy` cmdlet.

   Este exemplo reconfigura a cópia com falha do banco de dados chamado execkb no host "mva-RX200.NetApp.com" usando o backup mais recente nesse host.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb
```

   Este exemplo reconfigura a cópia com falha do banco de dados chamado execkb 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 as operações de restauração

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um 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 executar.

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito

- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Restore**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Cancelar operações de restauração para o banco de dados do Exchange

Você pode cancelar trabalhos de restauração que estão na fila.

Você deve estar logado como administrador do SnapCenter ou proprietário da tarefa para cancelar as operações de restauração.

Sobre esta tarefa

- Você pode cancelar uma operação de restauração em fila na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de restauração em execução.
- Você pode usar a GUI do SnapCenter, cmdlets do PowerShell ou os comandos CLI para cancelar as operações de restauração em fila.
- O botão **Cancelar trabalho** está desativado para operações de restauração que não podem ser canceladas.
- Se você selecionou **todos os membros desta função podem ver e operar em outros objetos membros** na página usuários/grupos ao criar uma função, você pode cancelar as operações de restauração em fila de outros membros enquanto usa essa função.

Passo

Execute uma das seguintes ações:

A partir 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 da atividade	1. Depois de iniciar a operação de restauração, clique no painel atividade para exibir as cinco operações mais recentes. 2. Selecione a operação. 3. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

Proteja o IBM DB2

Plug-in do SnapCenter para IBM DB2

Visão geral do plug-in do SnapCenter para IBM DB2

O plug-in do SnapCenter para o banco de dados IBM DB2 é um componente do lado do host do software NetApp SnapCenter que permite o gerenciamento da proteção de dados com reconhecimento de aplicativos 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 em seu ambiente SnapCenter.

- O SnapCenter 6,0 suporta IBM DB2 10,5 e posterior.
- O SnapCenter 6.0.1 suporta IBM DB2 9,7.x e posterior. Além disso, a partir do SnapCenter 6,0.1, o IBM DB2 no AIX é suportado.

O SnapCenter suporta configurações DB2 de instância única e várias instâncias. 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 node (DPF) não são suportados.

Quando o Plug-in para o banco de dados IBM DB2 é instalado, você pode 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 disco a disco para conformidade com os padrões.

O plug-in do SnapCenter para DB2 é compatível com NFS e SAN em layouts de storage de arquivos do ONTAP e do Azure NetApp.

VMDK ou layout de armazenamento virtual não é suportado.

O que você pode fazer usando o plug-in SnapCenter para IBM DB2

Quando você instala o Plug-in para o banco de dados IBM DB2 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.
- Criar backups.
- Restauração a partir de backups.
- Backups de clones.
- Agendar operações de backup.
- Monitore operações de backup, restauração e clone.
- Exibir relatórios para operações de backup, restauração e clone.

Plug-in do SnapCenter para recursos do IBM DB2

O SnapCenter se integra à aplicação plug-in e às tecnologias NetApp no sistema de storage. Para trabalhar com o plug-in para o banco de dados IBM DB2, use a interface gráfica do usuário do SnapCenter.

- * Interface gráfica unificada do usuário*

  A interface do SnapCenter fornece padronização e consistência em plug-ins e ambientes. A interface do SnapCenter permite concluir operações consistentes de backup, restauração e clone em plug-ins, usar relatórios centralizados, usar visualizações de painel rápidas, configurar controle de acesso baseado em funções (RBAC) e monitorar tarefas em todos os plug-ins.

- * Administração central automatizada*

  Você pode agendar operações de backup, configurar a retenção de backup baseada em política e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- **Tecnologia de cópia Snapshot NetApp sem interrupções**

  O SnapCenter usa a tecnologia de snapshot do NetApp com o Plug-in para Banco de dados IBM DB2 para fazer backup de recursos.

O uso do Plug-in para IBM DB2 também oferece os seguintes benefícios:

- Suporte a fluxos de trabalho de backup, restauração e clone
- Delegação de funções centralizada e segurança compatível com RBAC

  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 uso eficiente de espaço e pontuais para teste ou extração de dados usando a tecnologia NetApp FlexClone

  É necessária uma licença FlexClone no sistema de storage onde você deseja criar o clone.

- Suporte para o recurso instantâneo do grupo de consistência (CG) do ONTAP como parte da criação de backups.
- Funcionalidade de executar vários backups simultaneamente em vários hosts de recursos

  Em uma única operação, os snapshots são consolidados quando os recursos em um único host compartilham o mesmo volume.

- Capacidade de criar instantâneos usando comandos externos.
- Suporte para Linux LVM no sistema de arquivos XFS.

Tipos de storage compatíveis com o plug-in SnapCenter para IBM DB2

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e máquinas virtuais (VMs). Você deve verificar o suporte para seu tipo de storage antes de instalar o plug-in SnapCenter para IBM DB2.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados a FC • LUNs ligados ao iSCSI • Volumes conectados a NFS
VMware ESXi	• LUNs RDM conetados por um FC ou iSCSI ESXi HAScanning de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluído 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** para 1 para reexaminar somente os HBA listados em HBA_DRIVER_NAMES. • ISCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI • VMDKs em armazenamentos de dados NFS • VMDKs no VMFS criado • Volumes NFS conectados diretamente ao sistema convidado • Armazenamentos de dados da VVol em NFS e SAN O armazenamento de dados da VVol só pode ser provisionado com as Ferramentas do ONTAP para o VMware vSphere.

Mínimo de ONTAP Privileges necessário para o plug-in IBM DB2

Os ONTAP Privileges mínimos necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
  - event generate-AutoSupport-log
  - mostra o histórico de trabalhos
  - paragem do trabalho
  - lun
  - lun criar
  - lun criar

- lun criar
- eliminação lun
- lun igrop add
- lun igrop criar
- eliminação do agrupamento lun
- mudar o nome do grupo lun
- mudar o nome do grupo lun
- show de grupos de lun
- nós complementares de mapeamento de lun
- mapeamento lun criar
- eliminação do mapeamento lun
- mapeamento lun remove-reporting-nonos
- mostra de mapeamento lun
- modificação de lun
- movimentação de lun no volume
- lun offline
- lun online
- limpeza da reserva persistente de lun
- redimensionar lun
- série lun
- mostra lun
- regra adicional de política do SnapMirror
- regra de modificação de política do SnapMirror
- regra de remoção da política do SnapMirror
- SnapMirror policy show
- restauração de SnapMirror
- SnapMirror show
- SnapMirror show-history
- atualização do SnapMirror
- SnapMirror update-ls-set
- SnapMirror lista-destinos
- versão
- clone de volume criar
- show de clone de volume
- início da divisão do clone de volume
- paragem dividida clone volume
- criar volume

    - destruição de volume
    - clone de arquivo de volume criar
    - show-disk-use do arquivo de volume
    - volume off-line
    - volume online
    - modificação do volume
    - criar qtree de volume
    - eliminação de qtree de volume
    - modificação de qtree de volume
    - apresentação de qtree de volume
    - restrição de volume
    - apresentação do volume
    - criar instantâneo de volume
    - eliminar instantâneo do volume
    - modificação do instantâneo do volume
    - tempo de expiração do volume snapshot modify-SnapLock
    - mudar o nome do instantâneo do volume
    - restauração de snapshot de volume
    - restauração de arquivo de snapshot de volume
    - apresentação de instantâneo do volume
    - desmontar o volume
    - svm cifs
    - compartilhamento cifs de svm criar
    - exclusão de compartilhamento cifs de svm
    - apresentação do shadowcopy cifs de svm
    - exibição de compartilhamento cifs de svm
    - mostra cifs de svm
    - política de exportação de svm
    - criação de política de exportação de svm
    - exclusão da política de exportação do svm
    - regra de política de exportação de svm criar
    - a regra de política de exportação do svm é exibida
    - exibição da política de exportação do svm
    - svm iscsi
    - apresentação da ligação iscsi de svm
    - mostra o svm
- Comandos somente leitura: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior

- interface de rede
- mostra da interface de rede
- svm

Preparar sistemas de storage para replicação SnapMirror e SnapVault para IBM DB2

Você pode usar um plug-in do 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 disco a disco para conformidade com os padrões e outros fins relacionados à governança. Antes de executar essas tarefas, você deve configurar uma relação de proteção de dados entre os volumes de origem e destino e inicializar a relação.

O SnapCenter executa as atualizações para o SnapMirror e o SnapVault após concluir a operação de captura instantânea. As atualizações SnapMirror e SnapVault são executadas como parte da tarefa SnapCenter; não crie uma agenda ONTAP separada.

Se você estiver vindo para o SnapCenter de um produto NetApp SnapManager e estiver satisfeito com as relações de proteção de dados que configurou, ignore esta seção.

Uma relação de proteção de dados replica dados no storage primário (o volume de origem) para o storage secundário (o volume de destino). Ao inicializar a relação, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não suporta relações em cascata entre volumes SnapMirror e SnapVault (**Primary** > **Mirror** > **Vault**). Você deve usar relacionamentos de fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis de versão e como configurá-los, consulte "Documentação do ONTAP".

Estratégia de backup para IBM DB2

Defina uma estratégia de backup para o IBM DB2

Definir uma estratégia de backup antes de criar seus trabalhos de backup ajuda a ter os backups necessários para restaurar ou clonar seus recursos com êxito. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (rto) e objetivo do ponto de restauração (RPO) determinam em grande parte a sua estratégia de backup.

Sobre esta tarefa

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. Rto é o momento em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a era dos arquivos que precisam 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 de seus recursos.
2. Decida quantos trabalhos de cópia de segurança necessita.
3. Decida como nomear seus backups.
4. Decida se você deseja criar uma política baseada em cópia Snapshot para fazer backup de snapshots consistentes com aplicativos do banco de dados.
5. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção a longo prazo.
6. Determine o período de retenção dos snapshots no sistema de storage de origem e no destino do SnapMirror.
7. Determine se deseja executar quaisquer comandos antes ou depois da operação de backup e forneça um prescritor ou postscript.

Descoberta automática de recursos no host Linux

Os recursos são bancos de dados e instâncias do IBM DB2 no host Linux gerenciados pelo SnapCenter. Depois de instalar o plug-in do SnapCenter para IBM DB2, os bancos de dados do IBM DB2 de todas as instâncias desse host Linux são automaticamente descobertos e exibidos na página recursos.

Tipos de backups suportados

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 snapshot

Os backups baseados em cópias snapshot utilizam a tecnologia Snapshot NetApp para criar cópias on-line e somente leitura dos volumes nos quais os bancos de dados IBM DB2 residem.

Como o plug-in do SnapCenter para IBM DB2 usa snapshots de grupo de consistência

Você pode usar o plug-in para criar snapshots de grupo de consistência para grupos de recursos. Um grupo de consistência é um contentor que pode abrigar vários volumes para que você possa gerenciá-los como uma entidade. Um grupo de consistência são snapshots 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 **descontraído**. Você também pode ativar ou desativar a sincronização WAFL (Write Anywhere File Layout) durante uma operação consistente de snapshot em grupo. O WAFL Sync melhora o desempenho de um snapshot de grupo de consistência.

Como o SnapCenter gerencia o gerenciamento de backups de dados

O SnapCenter gerencia o gerenciamento de backups de dados nos níveis do sistema de storage e do sistema de arquivos.

Os instantâneos no armazenamento primário ou secundário e suas entradas correspondentes no catálogo IBM DB2 são excluídos com base nas configurações de retenção.

Considerações para determinar agendas de backup para IBM DB2

O fator mais crítico na determinação de um agendamento de backup é a taxa de alteração do recurso. Você pode fazer backup de um recurso muito usado a cada hora, enquanto você pode fazer backup de um recurso raramente usado uma vez por dia. Outros fatores incluem a importância do recurso para a sua organização, seu contrato de nível de serviço (SLA) e seu objetivo do ponto de restauração (RPO).

Os programas de backup têm duas partes, como segue:

- Frequência de backup (com que frequência os backups devem ser executados)

  A frequência de backup, também chamada de tipo de programação para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como hora, dia, semanal ou mensal.

- Programações de backup (exatamente quando os backups devem ser executados)

  As agendas de backup fazem parte de uma configuração de recurso ou grupo de recursos. Por exemplo, se você tiver um grupo de recursos que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas

Número de trabalhos de backup necessários para o IBM DB2

Os fatores que determinam o número de tarefas de backup de que você precisa 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 padrão de nomenclatura Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um carimbo de data/hora aos nomes de Snapshot 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 carimbo de data/hora.

Como alternativa, você pode especificar o formato do nome da captura Instantânea enquanto protege recursos ou grupos de recursos selecionando **usar formato de nome personalizado para cópia Instantânea**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do carimbo de hora é adicionado ao nome do instantâneo.

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 você possa executar operações de restauração e recuperação com sucesso.

Somente a recuperação manual do banco de dados é suportada.

Passos

1. Determine as estratégias de restauração suportadas para recursos do IBM DB2 adicionados manualmente
2. Determine 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 executar operações de restauração com êxito usando o SnapCenter. Existem 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 obtidos após o snapshot selecionado para restauração em tais 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 o IBM DB2 descoberto automaticamente

Você deve definir uma estratégia antes de executar operações de restauração com êxito usando o SnapCenter.

A restauração completa de recursos é a estratégia de restauração suportada para bancos de dados IBM DB2 automaticamente descobertos. Isso restaura todos os volumes, qtrees e LUNs de um recurso.

Tipos de operações de restauração para IBM DB2 descoberta automática

O plug-in do SnapCenter para IBM DB2 oferece suporte a SnapRestore de arquivo único e tipos de restauração de conexão e cópia para bancos de dados IBM DB2 descobertos automaticamente.

O SnapRestore de arquivo único é executado em ambientes NFS para os seguintes cenários:

- Se apenas a opção **Complete Resource** estiver selecionada
- Quando o backup selecionado é de um local secundário SnapMirror ou SnapVault e a opção **recurso completo** está selecionada

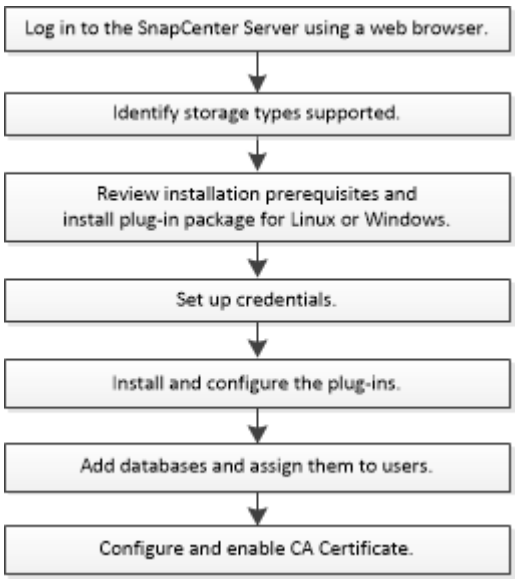
O SnapRestore de Arquivo único é executado em ambientes SAN para os seguintes cenários:

- Se apenas a opção **Complete Resource** estiver selecionada
- Quando o backup é selecionado em um local secundário do SnapMirror ou do SnapVault e a opção **recurso completo** está selecionada

Prepare-se para instalar o plug-in do SnapCenter para IBM DB2

Fluxo de trabalho de instalação do plug-in SnapCenter para IBM DB2

Você deve instalar e configurar o plug-in do SnapCenter para IBM DB2 se quiser proteger os bancos de dados do IBM DB2.



Pré-requisitos para adicionar hosts e instalar o pacote Plug-ins para Windows, Linux ou AIX

Antes de adicionar um host e instalar os pacotes de plug-in, você deve completar todos os requisitos. Plug-in do SnapCenter para IBM DB2 compatível com ambientes Windows, Linux e AIX.

- Você deve ter instalado o Java 11 em seu host.

  O IBM Java não é suportado.

- Para 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 do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host. O plug-in do SnapCenter para Microsoft Windows será implantado por padrão com o plug-in do IBM DB2 em hosts do Windows.
- O servidor SnapCenter deve ter acesso ao 8145 ou à porta personalizada do plug-in para o host IBM DB2.

Hosts do Windows

- Você deve ter um usuário de domínio com Privileges de administrador local com permissões de login local no host remoto.
- Ao instalar o plug-in para IBM DB2 em um host Windows, o plug-in SnapCenter 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 em seu host Windows.

  "Downloads Java para todos os sistemas operacionais"

  "Ferramenta de Matriz de interoperabilidade do 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 em seu host Linux.

  "Downloads Java para todos os sistemas operacionais"

  "Ferramenta de Matriz de interoperabilidade do NetApp"

- Para bancos de dados IBM DB2 que estão sendo executados em um host Linux, ao instalar o plug-in para IBM DB2, o plug-in SnapCenter para UNIX é instalado automaticamente.
- Você deve ter **bash** como o shell padrão para instalação do plug-in.

Comandos suplementares

Para executar um comando complementar no plug-in do SnapCenter para IBM DB2, você deve incluí-lo no arquivo *allowed_commands.config*.

- Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
- Localização 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 são sensíveis a maiúsculas e

minúsculas. Certifique-se de especificar o nome de caminho totalmente qualificado e incluir o nome de caminho entre aspas (") se ele contiver espaços.

Por exemplo:

comando: montar

comando: umount

Comando: "C: Arquivos de programas/comandos NetApp/sdcli.exe"

comando: myscript.bat

Se o arquivo *allowed_commands.config* não estiver presente, os comandos ou a execução de 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.

Configure sudo Privileges 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 de plug-in serão executados como um usuário não-root eficaz. Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se o umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro devem ter permissão de 555. Caso contrário, a instalação do plug-in pode falhar.
- Para o usuário não-root, certifique-se de que o nome do usuário não-root e do grupo do usuário devem ser os mesmos.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos de código de autenticação de mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

  Reinicie o serviço sshd depois de 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 o sudo Privileges para que o usuário não-root forneça acesso aos seguintes caminhos:

- /Home/*Linux_USER*/.SC_NetApp/SnapCenter_linux_host_plugin.bin
- /Custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/SnapCenter/spl/bin/spl

Passos

1. Faça 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 !visiblepw
Defaults: LINUX_USER !requiretty
```

Se você estiver tendo uma configuração RAC, juntamente 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**, que está localizado em:

- Se o servidor SnapCenter estiver instalado no host do Windows, o SnapCenter NetApp não será instalado no sistema operacional Windows.
- */opt/NetApp/SnapCenter/SnapManagerWeb/Repository/SC_UNIX_plugins_checksum.txt* se o servidor SnapCenter estiver instalado no host Linux.

O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Configure sudo Privileges para usuários não-root para host AIX

O SnapCenter 4,4 e posterior permite que um usuário não root instale o pacote de plug-ins do SnapCenter para AIX e inicie o processo de plug-in. Os processos de plug-in serão executados como um usuário não-root eficaz. Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se o umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro devem ter permissão de 555. Caso contrário, a instalação do plug-in pode falhar.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos de código de autenticação de mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

  Reinicie o serviço sshd depois de 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 o sudo Privileges para que o usuário não-root forneça acesso aos seguintes caminhos:

- /Home/*AIX_USER*/.SC_NetApp/SnapCenter_aix_host_plugin.bsx
- /Custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/SnapCenter/spl/bin/spl

Passos

1. Faça 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: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

Se você estiver tendo uma configuração RAC, juntamente 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**, que está localizado em:

- Se o servidor SnapCenter estiver instalado no host do Windows, o SnapCenter NetApp não será instalado no sistema operacional Windows.
- */opt/NetApp/SnapCenter/SnapManagerWeb/Repository/SC_UNIX_plugins_checksum.txt* se o servidor SnapCenter 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 do 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 do sistema host e requisitos de dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• .NET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet."

Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux

Antes de instalar o pacote de plug-ins do 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 • SUSE Linux Enterprise Server (SLES) Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto. Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do 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 raiz ou para um usuário não-root que tenha sudo Privileges para instalar e iniciar o processo de plug-in.

Prática recomendada: embora você tenha permissão para criar credenciais para Linux após implantar hosts e instalar plug-ins, a prática recomendada é criar credenciais após adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

  Você deve configurar as credenciais do Windows antes de instalar os plug-ins.

  Você deve configurar as credenciais com o Privileges 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 Privileges de administrador completo, será necessário atribuir pelo menos o grupo de recursos e Privileges de backup ao nome de usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Clique em **novo**.
4. Na página Credential (credencial), especifique as informações necessárias para configurar credenciais:

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para as credenciais.

Para este campo…	Faça isso…
Nome de utilizador	Introduza o nome de utilizador e a palavra-passe a utilizar para a 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 no qual você está instalando o plug-in do SnapCenter. Formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS_username* ◦ *Domain FQDN_username* • Administrador local (apenas para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é: *Nome de usuário* Não use aspas duplas (") ou backtick (') nas senhas. Você não deve usar os símbolos menos de (>) e exclamação (!) juntos em senhas. Por exemplo, lessthan!10, lessthan10You!, backtick'12.
Palavra-passe	Introduza a palavra-passe utilizada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que pretende utilizar.
Use sudo Privileges	Marque a caixa de seleção **Use sudo Privileges** se estiver criando credenciais para um usuário que não seja root. Aplicável apenas a usuários 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.

Configure o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite criar uma conta de serviço gerenciado de grupo (gMSA) que fornece gerenciamento automatizado de senha de conta de serviço a partir de uma conta de domínio gerenciado.

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 é um membro do domínio.

Passos

1. Crie uma chave raiz KDS para gerar senhas exclusivas para cada objeto em seu gMSA.
2. Para cada domínio, execute o seguinte comando do 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,…>
.. Execute `Get-ADServiceAccount` o comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Ative o módulo do ative Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando do 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 o host.

b. Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua o Privileges administrativo ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no servidor SnapCenter.

   O servidor SnapCenter 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.

Instale o plug-in do SnapCenter para IBM DB2

Adicione hosts e instale pacotes plug-in 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 servidor SnapCenter for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deve executar o seguinte:
  - Atualize para o Windows Server 2019 (versão de SO 17763,5936) ou posterior
  - Atualize para o Windows Server 2022 (versão de SO 20348,2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está

integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar 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 você estiver usando a conta de serviço gerenciado de grupo (gMSA), você deve configurar o gMSA com Privileges administrativo.

  "Configurar conta de serviço gerenciado de grupo no Windows Server 2016 ou posterior para IBM DB2"

Sobre esta tarefa

- Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Verifique se a guia **hosts gerenciados** está selecionada na parte superior.
3. Clique em **Add**.
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 cliente IBM DB2 e esse host pode estar em um sistema Windows ou em um sistema Linux.
Nome do host	Insira o nome do host de comunicação. Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no 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 exibir detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você forneceu. 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 instalar.

   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	Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido 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, você deve especificar a mesma porta. Caso contrário, a operação falha.
Caminho de instalação	O Plug-in para IBM DB2 é instalado no host cliente IBM DB2 e esse host pode estar em um sistema Windows ou em um sistema Linux. • Para o pacote de plug-ins do 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 do SnapCenter para Linux, o caminho padrão é /opt/NetApp/SnapCenter. Opcionalmente, você pode personalizar o caminho.

Para este campo…	Faça isso…
Ignorar as verificações de pré-instalação	Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	Para o host Windows, marque essa caixa de seleção se desejar usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in. Forneça o nome do gMSA no seguinte formato: O gMSA será usado como uma conta de serviço de logon apenas para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

   Se você não tiver selecionado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se o host 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 Linux) são validados de acordo com os requisitos mínimos. Se os requisitos mínimos não forem cumpridos, são apresentadas mensagens de erro ou de aviso adequadas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado no NetApp SnapCenter para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, será necessário atualizar o arquivo em ambos os nós.

8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirm and Submit**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós no cluster.

   A verificação de impressões digitais é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitorize o progresso da instalação.
   - Para o plug-in do Windows, os logs de instalação e atualização estão localizados em: *C: Plug-in do SnapCenter/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 de 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.

Instale pacotes de plug-ins do 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 PowerShell.

Antes de começar

Você deve ter feito 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 servidor SnapCenter, 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*. Em alternativa, pode também consultar o "Guia de referência de 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 do SnapCenter para IBM DB2 em hosts Linux usando a interface de linha de comando

Você deve instalar o plug-in do SnapCenter para o banco de dados IBM DB2 usando a interface de usuário (UI) do SnapCenter. Se o seu ambiente não permitir a instalação remota do plug-in a partir da IU do SnapCenter, você pode instalar o plug-in para o banco de dados IBM DB2 no modo console ou no modo silencioso usando a interface de linha de comando (CLI).

Antes de começar

- Você deve instalar o Plug-in para IBM DB2 Database em cada host Linux onde reside o cliente IBM DB2.
- O host Linux no qual você está instalando o plug-in do SnapCenter para o banco de dados IBM DB2 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 do NetApp"

- O plug-in do SnapCenter para o banco de dados IBM DB2 faz parte do pacote de plug-ins do SnapCenter para Linux. Antes de instalar o pacote de plug-ins do SnapCenter para Linux, você já deve ter instalado o SnapCenter em um host do Windows.

Sobre esta tarefa

Se os parâmetros não forem mencionados, o SnapCenter é instalado com valores padrão.

Passos

1. Copie o pacote de plug-ins do SnapCenter para o arquivo de instalação do Linux (SnapCenter_linux_host_plugin.bin) do repositório C:/NetApp/SnapCenter para o host onde você deseja instalar o plug-in para o IBM DB2.

   Você pode acessar esse caminho a partir do host onde o servidor SnapCenter 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 SMCore.
   - -DSERVER_IP especifica o endereço IP do servidor SnapCenter.
   - -DSERVER_HTTPS_PORT especifica a porta HTTPS do servidor SnapCenter.
   - -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 /<installation directory>/NetApp/SnapCenter/scc/etc/SC_SMS_Services.properties e, em seguida, adicione o parâmetro PLUGINS_ENABLED DB2:3,0.
5. Adicione o host ao servidor SnapCenter 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Monitore o status da instalação do Plug-in para IBM DB2

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito

- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
   a. Clique em **filtro**.
   b. Opcional: Especifique a data de início e fim.
   c. No menu suspenso tipo, selecione **Instalação 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 **Visualizar logs**.

Configurar certificado CA

Gerar arquivo CSR do 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 a CSR gerada. O certificado terá uma chave privada associada a ele.

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

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

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

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

Para configurações de cluster, o nome do cluster (FQDN de cluster virtual) e os respetivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome alternativo (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados CA

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 **Yes**, importe a chave privada e clique em **Next**.
Importar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

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

7. Repita o passo 5 para a pasta "Pessoal".

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia 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 **thumbprint**.
   d. Copie os carateres 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

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.

Configure o certificado CA com os serviços de plug-in do host do Windows

Você deve configurar o certificado CA com os serviços de plug-in host do Windows para ativar o certificado digital instalado.

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, 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"
   ```

Configure o certificado CA para o serviço de plug-ins IBM DB2 do SnapCenter 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. Altere a senha do keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Altere a senha para 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 depois de 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. Liste 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 de CA raiz e, em seguida, os certificados de CA intermediários.

Configurar o par de chaves assinadas pela CA para plug-in de armazenamento confiável

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. Liste 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. Liste os certificados adicionados no keystore.

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

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

   A senha padrão do keystore 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 espaço ou
   carateres 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 com a chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o plug-in trust-store.

Configurar a lista de revogação de certificados (CRL) para plug-ins do SnapCenter

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 SnapCenter é 'opt/NetApp/snapcenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties contra a chave CRL_PATH.

   Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Configure o certificado CA para o serviço de plug-ins IBM DB2 do SnapCenter 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 Plug-ins 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. Altere 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 por seu caminho completo.

   C: Arquivos de programas/<jdk_version>/keytool.exe" -storepasswd -keystore keystore.jks

3. Altere a senha para 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*.

4. Reinicie o serviço depois de 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. Liste 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 de CA raiz e, em seguida, os certificados de CA intermediários.

Configurar o par de chaves assinadas pela CA para plug-in de armazenamento confiável

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. Liste 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 -destinkeystore keystore.jks -deststoretype JKS

5. Liste os certificados adicionados no keystore.

   keytool -list -v -keystore keystore.jks

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da 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

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

   Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o plug-in trust-store.

Configurar a lista de revogação de certificados (CRL) para plug-ins do SnapCenter

Sobre esta tarefa

- Para transferir o ficheiro CRL mais recente para o certificado CA relacionado, "Como atualizar o arquivo

de lista de revogação de certificados no certificado da CA do SnapCenter"consulte .

- 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* contra a chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

   Os certificados recebidos serão verificados em relação a cada CRL.

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet RUN *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando as *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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- * * Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da 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 são concluídas com êxito.

Preparar-se para a proteção de dados

Pré-requisitos para usar o plug-in SnapCenter para IBM DB2

Antes de usar o plug-in do SnapCenter para IBM DB2, o administrador do SnapCenter deve instalar e configurar o servidor SnapCenter e executar as tarefas de pré-requisito.

- Instalar e configurar o servidor SnapCenter.
- Inicie sessão no servidor SnapCenter.
- Configure o ambiente SnapCenter adicionando conexões do sistema de storage e criando credenciais, se aplicável.
- Instale o Java 11 em seu host Linux ou Windows.

  Você deve definir o caminho Java na variável caminho ambiental da máquina host.

- Configure o SnapMirror e o SnapVault, se quiser 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 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 são normalmente bancos de dados IBM DB2 que você faz backup ou clonar com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host.

  Quando você executa uma operação em um grupo de recursos, executa essa operação nos recursos definidos no grupo de recursos de acordo com a programação especificada 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 programados para recursos únicos e grupos de recursos.

- As políticas especificam a frequência do backup, a replicação, os scripts e outras caraterísticas 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 quando você executa um backup sob demanda para um único recurso.

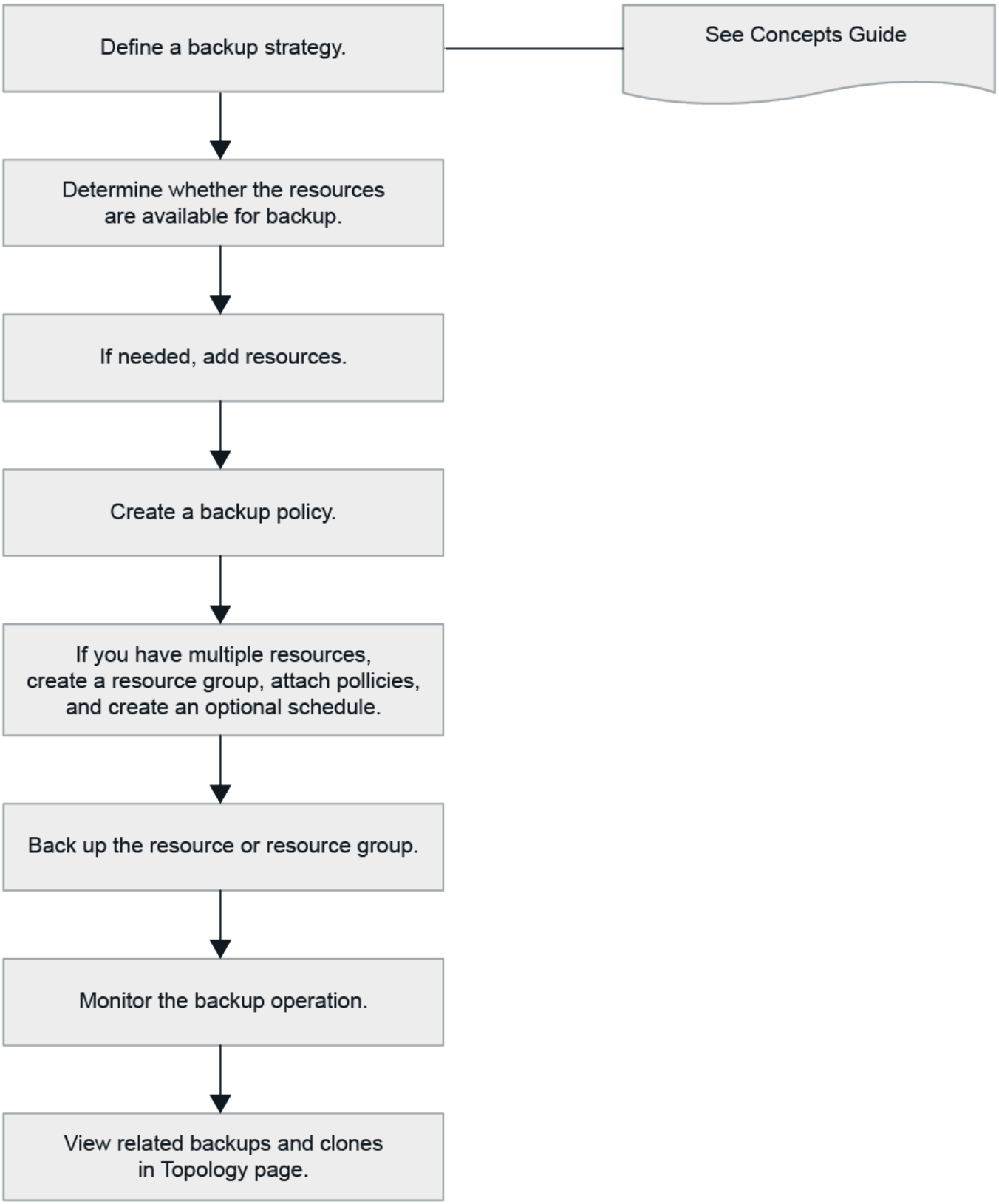
Pense em um grupo de recursos como definindo o que você quer proteger e quando você quer protegê-lo em termos de dia e tempo. Pense em uma política como definir como você deseja protegê-la. Se você estiver fazendo backup de todos os bancos de dados, por exemplo, poderá criar um grupo de recursos que inclua todos os bancos de dados no host. Em seguida, você pode anexar duas políticas ao grupo de recursos: Uma política diária e uma política por hora. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diariamente.

Faça backup dos recursos do IBM DB2

Faça 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 de bancos de dados para backup, gerenciamento de políticas de backup, criação de grupos de recursos e inclusão 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 clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell. "Guia de referência de cmdlet do software SnapCenter".

Descubra os bancos de dados automaticamente

Os recursos são bancos de dados IBM DB2 no host Linux gerenciados pelo SnapCenter. Você pode adicionar os recursos a grupos de recursos para executar operações de proteção de dados depois de descobrir os bancos de dados do IBM DB2 disponíveis.

Antes de começar

- Você já deve ter concluído tarefas como instalar o servidor SnapCenter, adicionar hosts e configurar as conexões do sistema de armazenamento.
- O plug-in do SnapCenter para IBM DB2 não oferece suporte à descoberta automática dos recursos residentes em ambientes virtuais RDM/VMDK. Você deve fornecer as informações de storage para ambientes virtuais e adicionar os bancos de dados manualmente.

Sobre esta tarefa

- Depois de instalar o plug-in, todos os bancos de dados nesse host Linux são automaticamente descobertos e exibidos na página recursos.
- Somente bancos de dados são auto-descobertos.

Os recursos descobertos automaticamente não podem ser modificados ou excluídos.

Passos

1. No painel de navegação à esquerda, clique em **Resources** 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 selecione o nome do host.

   Em seguida, pode clicar em* * para fechar o painel do filtro.

4. Clique em **Atualizar recursos** para descobrir os recursos disponíveis no host.

   Os recursos são exibidos juntamente 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, então não protegido será exibido na coluna Estado geral.
   - Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, e se não houver operação de backup executada, o Backup não executado será exibido na coluna Estado geral. O status mudará para Backup failed ou Backup successful com base no último status de backup.

Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

Adicione recursos manualmente ao host do plug-in

A deteção automática não é suportada no host Windows. Você deve adicionar instâncias DB2 e recursos de banco de dados manualmente.

Antes de começar

- Você deve ter concluído tarefas como instalar o servidor SnapCenter, adicionar hosts e configurar conexões do sistema de armazenamento.

Sobre esta tarefa

A deteção manual não é suportada para as seguintes configurações:

- Layouts RDM e VMDK

Passos

1. No painel de navegação à esquerda, selecione **Resources** e, em seguida, selecione o plug-in SnapCenter 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	Insira o nome do host.
Tipo	Selecione banco de dados ou instância.
Instância	Especifique o nome da instância, que é o pai do banco de dados.
Credenciais	Selecione as credenciais ou adicione informações para a credencial. Isso é opcional.

4. Na página fornecer espaço físico 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 valor de chave personalizados para o plug-in IBM DB2
6. Revise o resumo e clique em **Finish**.

   Os bancos de dados são exibidos juntamente com informações como o nome do host, grupos e políticas de recursos associados e status geral

Se você quiser fornecer aos usuários acesso a recursos, você deve atribuir os recursos aos usuários. Isso permite que os usuários executem as ações para as quais eles têm permissões nos ativos que são atribuídos a eles.

"Adicione um usuário ou grupo e atribua funções e ativos"

Depois de adicionar os bancos de dados, você pode modificar os detalhes do banco de dados do IBM DB2.

Criar políticas de backup para o IBM DB2

Antes de usar o SnapCenter para fazer backup de recursos do IBM DB2, você deve criar uma política de backup para o grupo de recursos ou recursos que deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e retém backups.

Antes de começar

- Você precisa 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 precisa se preparar para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, configurar conexões do sistema de storage e adicionar recursos.
- O administrador do SnapCenter deve ter atribuído os SVMs para os volumes de origem e destino a você se estiver replicando snapshots em um espelho ou cofre.

  Além disso, você pode especificar as 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 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio de instantâneos impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na política.
  - Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

As configurações do SnapLock primário são gerenciadas na política de backup do SnapCenter e as configurações do SnapLock secundário são gerenciadas pelo ONTAP.

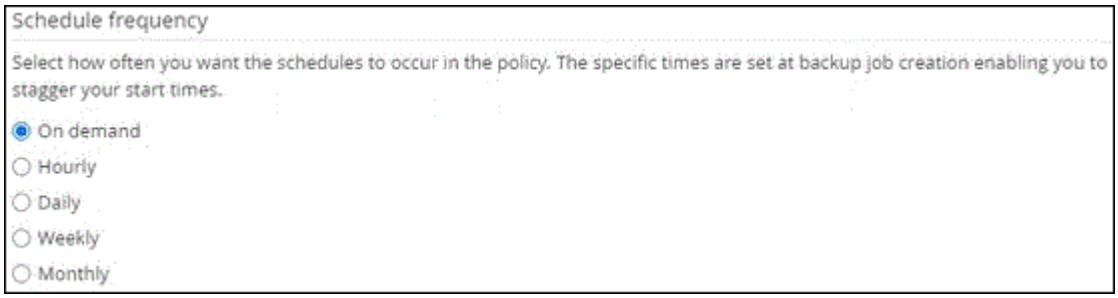
Passos

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 a descrição da política.
5. Na página tipo de política, execute o seguinte:
   a. Selecione o tipo de armazenamento.
   b. Na seção **Configurações personalizadas de backup**, forneça quaisquer configurações específicas de backup que tenham que ser passadas para o formato de valor de chave do plug-in.

      Você pode fornecer vários valores-chave a serem passados para o plug-in.

6. Na página Snapshot, especifique o tipo de agendamento selecionando **On Demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.

Você pode especificar a programação (data de início, data de término e frequência) para a operação de backup enquanto cria 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 programações de backup a cada política.



Se você tiver agendado para as 2:00 da manhã, o horário não será acionado durante o horário de verão (DST).

7. Na seção Configurações de instantâneos, especifique o número de instantâneos que você deseja manter.

Se você quiser…	Então…
Mantenha um certo número de instantâneos	Selecione **Copies to keep** e especifique o número de instantâneos que deseja manter. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro.

Para backups baseados em cópias Snapshot, defina a contagem de retenção para 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção pode falhar porque o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino.

8. Na página retenção e backup, especifique as configurações de retenção para o tipo de backup e o tipo de agendamento selecionado na página tipo de backup:
9. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas

Um grupo de recursos é o contentor ao qual você deve adicionar recursos que deseja fazer backup e proteger. Um grupo de recursos permite fazer 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 tarefa de proteção de dados que deseja executar.

Sobre esta tarefa

- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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	Introduza um nome para o grupo de recursos. O nome do grupo de recursos não deve exceder 250 carateres.
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.
Use o formato de nome personalizado para cópia instantânea	Marque essa 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 carimbo de data/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 **Resource Type**.

   Isso ajuda a filtrar informações na tela.

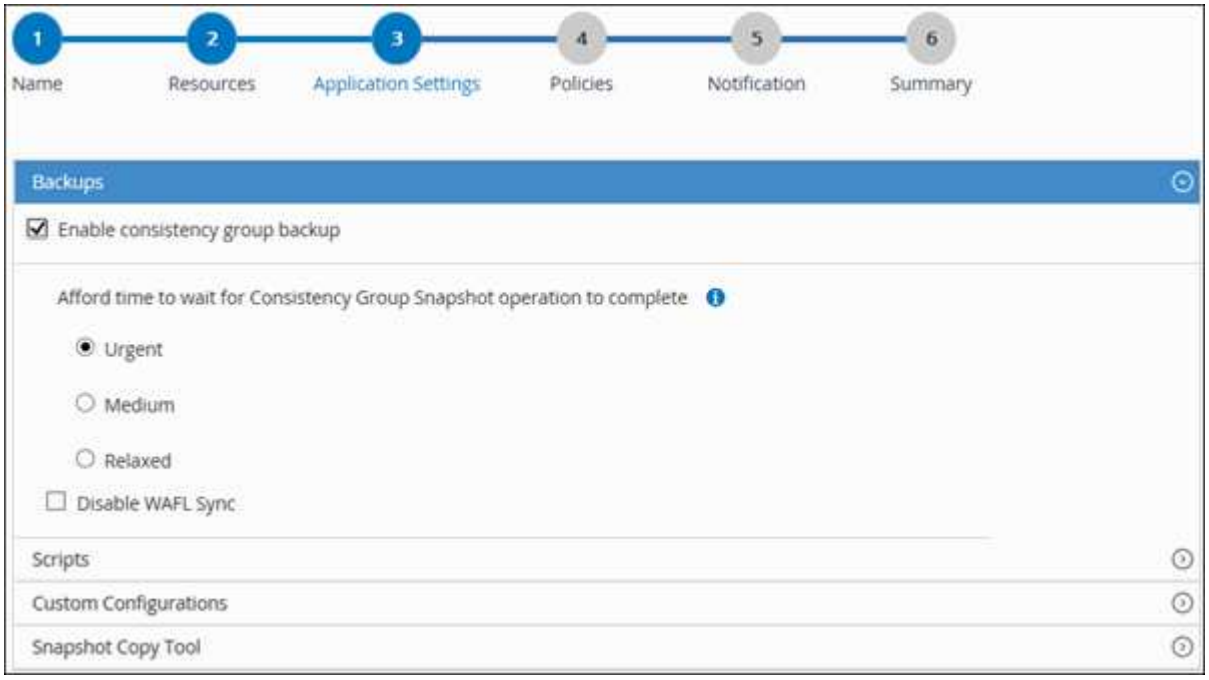
5. Selecione os recursos na seção **recursos disponíveis** e clique na seta para a direita para movê-los para a seção **recursos selecionados**.
6. Na página Configurações do aplicativo, faça o seguinte:

   a. Clique na seta **backups** para definir opções adicionais de backup:

      Ative o backup do grupo de consistência e execute as seguintes tarefas:

Para este campo…	Faça isso…
Tenha tempo para esperar que a operação de snapshot do Grupo de consistência seja concluída	Selecione **urgente**, **Médio** ou **relaxado** para especificar o tempo de espera para que a operação de snapshot seja concluída. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a 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 quiesce, snapshot e unquiesce. Também pode introduzir os pré comandos a serem executados antes de sair em caso de falha.

b. Clique na seta **Custom Configurations** (Configurações personalizadas) e insira os pares de valor de chave personalizados necessários para todas as operações de proteção de dados usando esse recurso.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_ENABLE	(Y/N)	Permite que a gestão do registo de arquivo elimine os registos de arquivo.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_RETENÇÃO	number_of_days	Especifica o número de dias em que os logs de arquivo são mantidos. Esta definição tem de ser igual ou superior a NTAP_SNAPSHOT_ RETENÇÕES.
ARCHIVE_LOG_DIR	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs do arquivo.
ARCHIVE_LOG_EXT	extensão_ficheiro	Especifica o comprimento da extensão do arquivo de log do arquivo. Por exemplo, se o log de arquivo 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.
ARCH ARCHIVE_LOG_RECURSIVE_ SE	(Y/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs do arquivo 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 banco de dados IBM DB2 registrado como um plug-in centralizado do Windows.

c. Clique na seta **Snapshot Copy Tool** 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, essa opção não é aplicável.	Selecione **SnapCenter com consistência do sistema de arquivos**.
SnapCenter para criar um instantâneo de nível de storage	Selecione **SnapCenter sem consistência do sistema de arquivos**.

Se você quiser…	Então…
Para inserir o comando a ser executado no host para criar cópias snapshot.	Selecione **Other** e, em seguida, digite 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 programações para políticas selecionadas.

   b. Na coluna Configurar agendas, clique em + para a política que deseja configurar.

   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e clique em **OK**.

      Onde, policy_name é o nome da política selecionada.

      As programações configuradas são listadas na coluna **programações aplicadas**.

   As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas 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 **Finish**.

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 Administrador da infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estão em andamento.

  As instalações de plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento, pois 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 do sistema de armazenamento devem ser exclusivos.

  O SnapCenter não é compatível com vários sistemas de storage com o mesmo nome em clusters diferentes. Cada sistema de storage com suporte do SnapCenter deve ter um nome exclusivo e um endereço IP de 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 servidor SnapCenter.

   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 do 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 o Windows, o plug-in DB2 usará o caminho padrão para a pasta SQLLIB:

   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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Faça backup de bancos de dados DB2

Fazer backup de um banco de dados inclui estabelecer uma conexão com o servidor SnapCenter, 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 uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.
- Para a operação de backup baseada em cópia Snapshot, certifique-se de que todos os bancos de dados do locatário estejam válidos e ativos.
- Para comandos pré e POST para operações quiesce, Snapshot e unquiesce, você deve verificar se os comandos existem na lista de comandos disponível no host plug-in dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização padrão no host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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, em seguida, selecione o nome do host e o tipo de recurso para filtrar os recursos. Em seguida, pode selecionar para fechar o painel de filtro.
3. Selecione o recurso que você deseja fazer backup.
4. Na página recurso, selecione **Use o formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.
5. Na página Configurações do aplicativo, faça o seguinte:
   - Selecione a seta **backups** para definir opções adicionais de backup:

     Ative o backup do grupo de consistência, se necessário, e execute as seguintes tarefas:

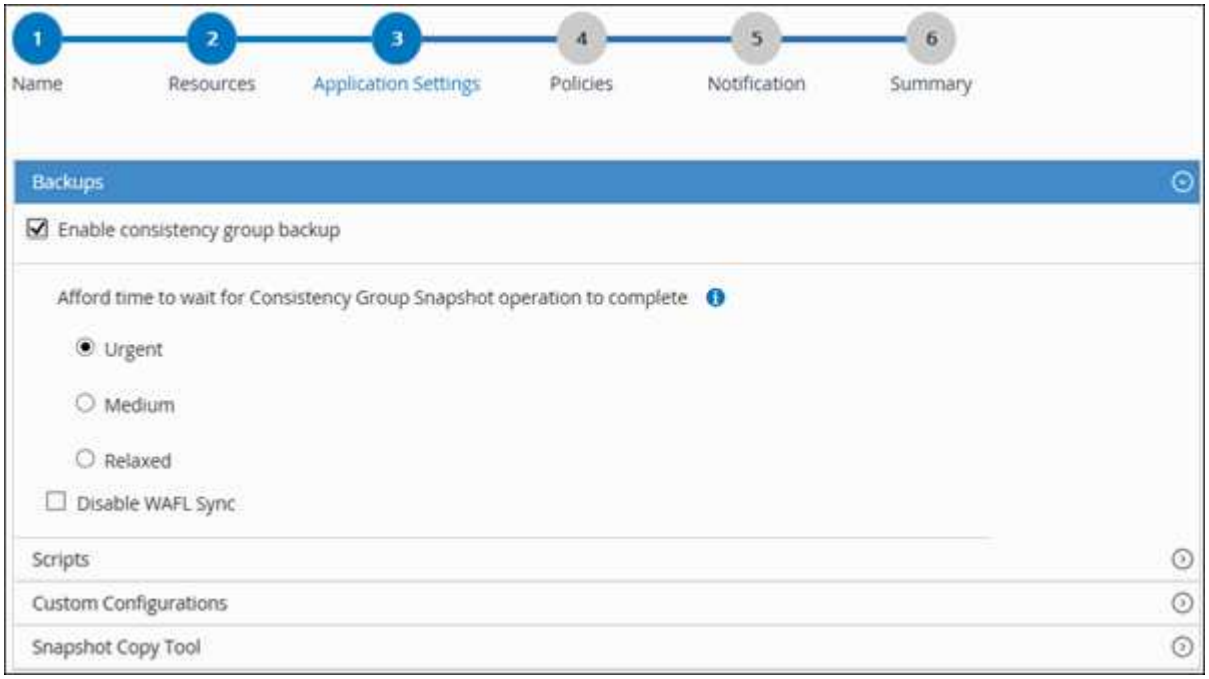
Para este campo…	Faça isso…
Tenha tempo para esperar a conclusão da operação "Consistency Group Snapshot"	Selecione **urgente**, **Médio** ou **relaxado** para especificar o tempo de espera para que a operação Snapshot termine. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL.

   - Selecione a seta **Scripts** para executar comandos pré e POST para operações quiesce, Snapshot e unquiesce.

     Você também pode executar pré-comandos antes de sair da operação de backup. Os Prescripts e postscripts são executados no servidor SnapCenter.
   - Selecione a seta **Custom Configurations (Configurações personalizadas) e, em seguida, insira os pares de valores personalizados necessários para todos os trabalhos que usam esse recurso.
   - Selecione a seta **Snapshot Copy Tool** para selecionar a ferramenta para criar instantâneos:

Se você quiser…	Então…
SnapCenter para criar um Snapshot no nível de storage	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 instantâneo	Selecione **SnapCenter com consistência do sistema de arquivos**.
Para inserir o comando para criar uma captura Instantânea	Selecione **Other** e, em seguida, digite o comando para criar uma captura Instantânea.



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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Selecione + * * na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e selecione **OK**.

      policy_name é o nome da política selecionada.

   As programações configuradas são listadas na coluna agendas aplicadas.

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 **Finish**.

   A página de topologia de recursos é exibida.

9. Selecione **fazer uma cópia de segurança 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. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.
    - Nas configurações do MetroCluster, o SnapCenter pode não ser capaz de detetar uma relação de proteção após um failover.

      Para obter informações, consulte: "Não é possível detetar a relação SnapMirror ou SnapVault após o failover do MetroCluster"

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

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

   É apresentado o aviso de nome de utilizador e palavra-passe.

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 a base 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 da tarefa (em execução, concluída 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 da tarefa de backup, como ID do backup, nome do backup para executar a operação de restauração ou clone 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*. Em alternativa, pode também consultar o "Guia de referência de 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 uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, 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 uma programação configurada, os backups ocorrerão automaticamente de acordo com a programação.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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 selecionando a tag. Em seguida, pode 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. Monitorize 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. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado correspondente das operações:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- 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 a que apenas as operações de cópia de segurança sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Backup**.
   d. Na lista suspensa **Status**, selecione o status da cópia de segurança.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.

   Embora o status do trabalho de backup seja exibido , quando você clica nos detalhes do trabalho, você pode ver que algumas das tarefas secundárias da operação de backup ainda estão em andamento ou marcadas com sinais de aviso.

5. Na página Detalhes da tarefa, clique em **Exibir logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Monitore operações de proteção de dados em bancos de dados IBM DB2 no painel atividade

O painel atividade exibe as cinco operações mais recentes executadas. O painel atividade também é exibido quando a operação foi iniciada e o status da operação.

O painel atividade exibe informações sobre operações de backup, restauração, clone e backup agendadas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 da tarefa**.

Cancelar operações de backup para IBM DB2

Você pode cancelar as operações de backup que estão na fila.

O que você vai precisar

- Você deve estar logado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de cópia de segurança em execução.
- Você pode usar os comandos GUI, cmdlets do SnapCenter ou CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** está desativado 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 em fila de outros membros enquanto usa essa função.

Passos

1. Execute uma das seguintes ações:

A partir 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 da atividade	a. Depois de iniciar a operação de backup, clique em no painel atividade para exibir as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

A operação é cancelada e o recurso é revertido para o estado anterior.

Veja os backups e clones do IBM DB2 na página topologia

Ao se preparar para fazer backup ou clonar um recurso, talvez seja útil exibir uma representação gráfica de todos os backups e clones no storage primário e secundário.

Sobre esta tarefa

Você pode revisar os ícones a seguir na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no storage primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups e clones disponíveis no storage primário.
- Exibe o número de backups e clones espelhados no storage secundário usando a tecnologia SnapMirror.
- Exibe o número de backups e clones replicados no storage secundário usando a tecnologia SnapVault.

O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou backups 6 usando uma política para reter apenas 4 backups, o número de backups exibidos é 6.

Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

Na página topologia, você pode ver todos os backups e clones disponíveis para o grupo de recursos ou recursos selecionado. Você pode visualizar os detalhes desses backups e clones e, em seguida, selecioná-los para executar operações de proteção de dados.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o recurso ou o 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 de 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 baseados em cópia Snapshot.

   Clicar no botão **Refresh** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clique no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Um horário semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo é espalhado por vários volumes, o tempo de expiração do SnapLock para o backup será o tempo de expiração do SnapLock mais longo definido para um snapshot em um volume. O tempo de expiração mais longo do SnapLock é recuperado do ONTAP.

   Após o backup sob demanda, clicando no botão **Refresh** atualiza os detalhes do backup ou clone.

5. No modo de 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 um 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 estão no armazenamento secundário.

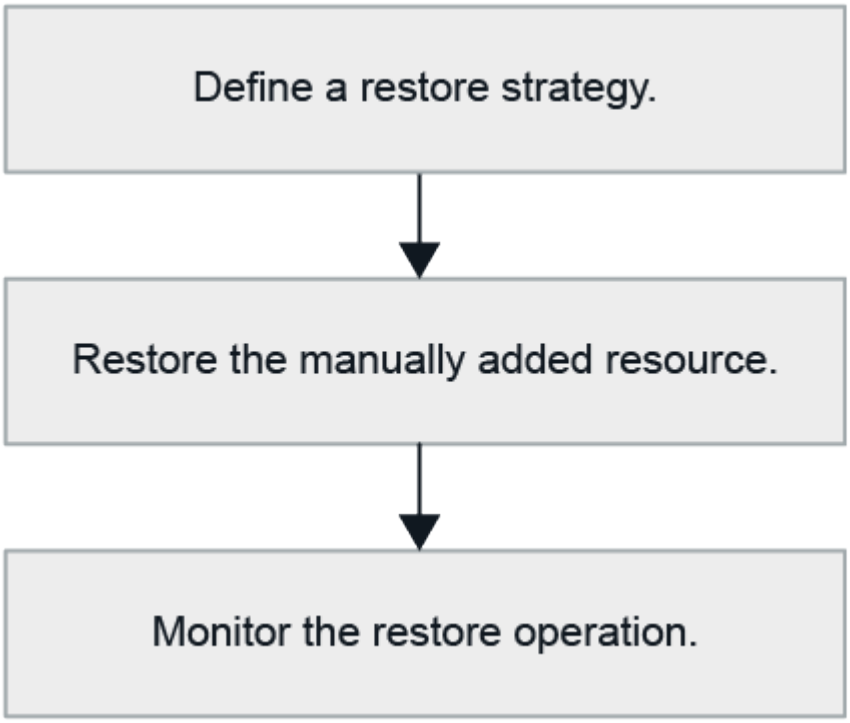
7. Se quiser excluir um clone, selecione-o na tabela e clique em .
8. Se quiser dividir um clone, selecione-o na tabela e clique em .

Restaure o IBM DB2

Restaure o fluxo de trabalho

O fluxo de trabalho de restauração e recuperação inclui Planejamento, execução das 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 clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre cmdlets do PowerShell.

"Guia de referência de cmdlet do software SnapCenter".

Restaurar um backup de recursos 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 dos grupos de recursos ou recursos.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos pré-restauração, pós restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização 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 a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com o tipo, host, grupos de recursos e políticas associados e status.

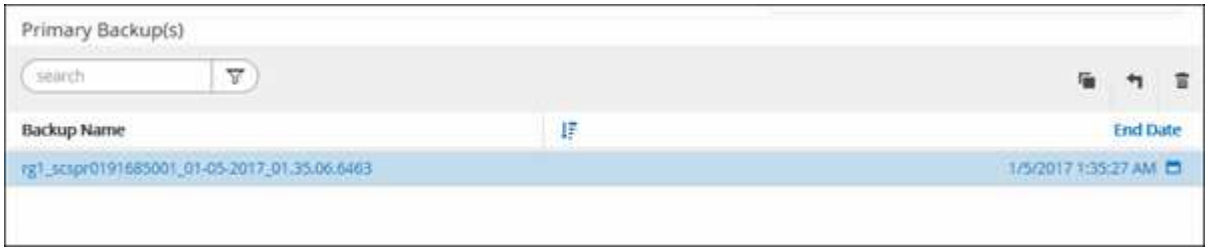
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, ""não protegido"" é exibido na coluna Estado geral. Isso pode significar que o recurso não está protegido ou que o recurso foi protegido 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 do recurso é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Na tabela de backup principal, selecione o backup do qual você deseja restaurar e clique em * * .



6. Na página Restaurar escopo, selecione **recurso completo**.

   a. Se você selecionar **Complete Resource**, todos os volumes de dados configurados do banco de dados IBM DB2 serão restaurados.

      Se o recurso contiver volumes ou qtrees, os instantâneos obtidos 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.

      Pode selecionar vários LUNs.

      Se você selecionar **All**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.

7. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar um trabalho de restauração.
8. Na página Post OPS, insira os comandos mount e POST Restore para serem executados após a execução de 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 **Finish**.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Depois de terminar

A recuperação só é possível se o status Rollforward estiver no status "DB pendente". Este status é aplicável a bancos de dados DB2 com Registro de arquivo ativado.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 existem 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 29th 2015 de janeiro a 3rd 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 dados do backup usando o cmdlet Restore-SmBackup.

> <instance_name> é para o recurso de instância DB2 descoberta manualmente e UID: <instance_name> é para o recurso de <databse_name> banco de dados IBM DB2. Você pode obter o ResourceID do 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Restaure e recupere 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 dos grupos de recursos ou recursos.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos pré-restauração, pós restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização 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 descoberta automática, a restauração é suportada com SFSR.
- A recuperação automática não é suportada.
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente 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.

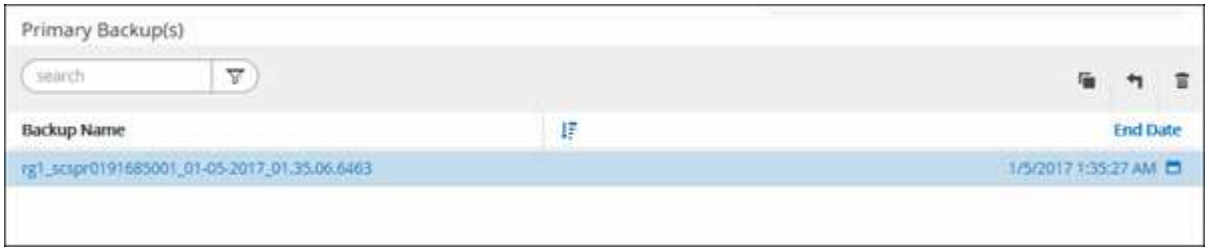
   Se o recurso não estiver protegido, ""não protegido"" é exibido na coluna Estado geral. Isso pode significar

que o recurso não está protegido ou que o recurso foi protegido 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 do recurso é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Na tabela de backup principal, selecione o backup do qual você deseja restaurar e clique em * * .



6. Na página Restaurar escopo, selecione **recurso completo** para restaurar os volumes de dados configurados do banco de dados IBM DB2.
7. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar um trabalho de restauração.

   Os comandos de desmontagem não são necessários para recursos detetados automaticamente.

8. Na página Post OPS, insira os comandos mount e POST Restore para serem executados após a execução de um trabalho de restauração.

   Os comandos de montagem não são necessários para recursos detetados 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 **Finish**.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Depois de terminar

A recuperação só é possível se o status Rollforward estiver no status "DB pendente". Este status é aplicável a bancos de dados DB2 com Registro de arquivo ativado.

Monitorar operações de restauração do IBM DB2

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um 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 executar.

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Restore**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Clonar backups de recursos do IBM DB2

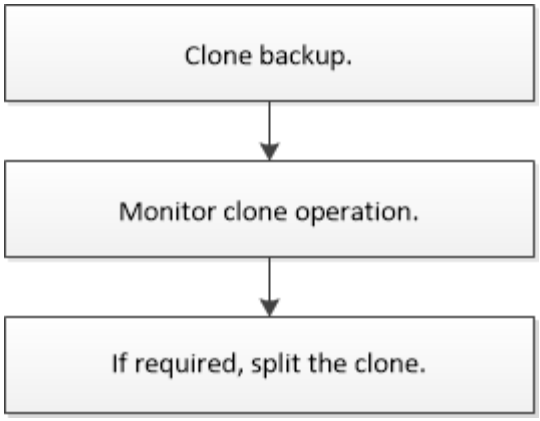
Fluxo de trabalho clone

O fluxo de trabalho do clone inclui a execução da operação de clone e o monitoramento da 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 de aplicativos
  - 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 clone:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre cmdlets do PowerShell.

Depois de terminar

Após clonar os recursos DB2 automaticamente descobertos, o recurso clonado é marcado como recurso manual. Clique em **Refresh Resources** (Atualizar recursos*) para recuperar o recurso clonado DB2. Quando você exclui o clone, o armazenamento e o host também são limpos.

Se você não atualizar os recursos após a operação de clone 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 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 storage (SVM).
- Ao criar um clone para DB2 em um host alternativo, você deve criar uma estrutura de diretório n-1 para o caminho de montagem clone igual ao caminho de montagem original no outro host. O caminho de montagem deve ter permissão de execução *755*.
- Para comandos pré-clone ou pós-clone, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização 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 limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage

deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com informações como tipo, host, grupos e políticas de recursos associados e status.

3. Selecione o grupo de recursos ou recursos.

   Você deve selecionar um recurso se selecionar um grupo de recursos.

   A página de topologia do grupo de recursos ou recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Selecione o backup de dados na 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 de clone de destino	Insira o ID da instância do clone DB2 de destino para clonar dos backups existentes. Isso se aplica apenas ao recurso do tipo de storage do ANF.
Nome do clone alvo	Introduza o nome do clone. Isso é aplicável apenas para o recurso de banco de dados DB2.
Endereço IP de exportação NFS	Insira endereços IP ou os nomes de host nos quais os volumes clonados serão exportados. Isso é aplicável apenas ao recurso do tipo de storage NFS.
Taxa de transferência máx. Do pool de capacidade (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. Digite os comandos para pré-clone ou pós-clone que devem ser executados antes ou depois da operação clone, respetivamente.

- Comando pre clone: Exclua bancos de dados existentes com o mesmo nome
- Comando Post clone: Verifique um banco de dados ou inicie um banco de dados.

b. Digite o comando mount para montar um sistema de arquivos em um host.

Monte o comando 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 **Finish**.
10. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Depois de terminar

Após clonar os recursos DB2 automaticamente descobertos, o recurso clonado é marcado como recurso manual. Clique em **Refresh Resources** (Atualizar recursos*) para recuperar o recurso clonado DB2. Quando você exclui o clone, o armazenamento e o host também são limpos.

Se você não atualizar os recursos após a operação de clone 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 servidor SnapCenter 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 clone a partir de um backup existente usando o cmdlet New-SmClone.

   Este exemplo cria um clone a partir 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. Exiba o status da tarefa clone usando o cmdlet Get-SmCloneReport.

   Este exemplo exibe um relatório de clone para a ID de tarefa especificada:

```
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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Monitorar operações de clone do IBM DB2

Você pode monitorar o andamento das operações de clone do SnapCenter usando a página tarefas. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista para que apenas operações de clone sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Divida um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido torna-se independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clones em um clone intermediário.

  Por exemplo, depois de criar clone1 a partir de um backup de banco de dados, você pode criar um backup de clone1 e clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e não é possível executar a operação de divisão de clones no clone1. No entanto, você pode executar a operação de divisão de clones no clone2.

  Depois de dividir clone2, você pode executar a operação de divisão de clones no clone1 porque clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e as tarefas de clone do clone são excluídas.
- Para obter informações sobre limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .
- Certifique-se de que o volume ou o agregado no sistema de storage esteja on-line.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página **recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicativos 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 do recurso é exibida.

4. No modo de 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 deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

   A operação de divisão de clones deixa de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clones e tentar novamente a operação de divisão de clones.

   Se você quiser um tempo de enquete mais longo 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 que o SMCore busque o status da operação de divisão de clones. O valor é em milissegundos e o valor padrão é de 5 minutos.

   Por exemplo:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   A operação de inicialização dividida de clone falhará se o backup, a restauração ou outra divisão de clones estiver em andamento. Você deve reiniciar a operação de divisão de clones somente depois que as operações em execução estiverem concluídas.

Informações relacionadas

"O clone ou a verificação do SnapCenter falha com o agregado não existe"

Exclua ou divida clones do banco de dados IBM DB2 após a atualização do SnapCenter

Após a atualização para o SnapCenter 4,3, você não verá mais os clones. Você pode excluir o clone ou dividir os clones da página topologia do recurso a partir do qual os clones foram criados.

Sobre esta tarefa

Se você quiser localizar o espaço físico 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-sprotectresource.
4. Selecione o recurso pai na página recursos.

   A página de topologia do recurso é exibida.

5. Na visualização Gerenciar cópias, selecione os clones nos sistemas de storage primário ou secundário (espelhado ou replicado).
6. Selecione os clones e clique para excluir clones ou clique para dividir os clones.

7. Clique em **OK**.

Proteja o PostgreSQL

Plug-in SnapCenter para PostgreSQL

Visão geral do plug-in do SnapCenter para PostgreSQL

O cluster do SnapCenter Plug-in para PostgreSQL é um componente do lado do host do software NetApp SnapCenter que permite o gerenciamento de clusters do PostgreSQL com reconhecimento de aplicativos. O cluster Plug-in para PostgreSQL automatiza o backup, a restauração e a clonagem de clusters PostgreSQL em seu ambiente SnapCenter.

O SnapCenter suporta configurações de cluster único e multi cluster 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 é instalado, você pode 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 disco a disco para conformidade com os padrões.

O plug-in do SnapCenter para PostgreSQL é compatível com NFS e SAN em layouts de storage de arquivos do ONTAP e do Azure NetApp.

O VMDK ou o layout de armazenamento virtual são suportados.

O que você pode fazer usando o plug-in SnapCenter para PostgreSQL

Ao instalar o cluster Plug-in para 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.
- Criar backups.
- Restauração a partir de backups.
- Backups de clones.
- Agendar operações de backup.
- Monitore operações de backup, restauração e clone.
- Exibir relatórios para operações de backup, restauração e clone.

Plug-in do SnapCenter para recursos PostgreSQL

O SnapCenter se integra à aplicação plug-in e às tecnologias NetApp no sistema de storage. Para trabalhar com o Plug-in para cluster PostgreSQL, use a interface gráfica do usuário do SnapCenter.

- * Interface gráfica unificada do usuário*

A interface do SnapCenter fornece padronização e consistência em plug-ins e ambientes. A interface do SnapCenter permite concluir operações consistentes de backup, restauração e clone em plug-ins, usar relatórios centralizados, usar visualizações de painel rápidas, configurar controle de acesso baseado em funções (RBAC) e monitorar tarefas em todos os plug-ins.

- * Administração central automatizada*

  Você pode agendar operações de backup, configurar a retenção de backup baseada em política e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- **Tecnologia de cópia Snapshot NetApp sem interrupções**

  O SnapCenter usa a tecnologia de snapshot do NetApp com o cluster Plug-in para PostgreSQL para fazer backup de recursos.

Usar o Plug-in para PostgreSQL também oferece os seguintes benefícios:

- Suporte a fluxos de trabalho de backup, restauração e clone
- Delegação de funções centralizada e segurança compatível com RBAC

  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 uso eficiente de espaço e pontuais para teste ou extração de dados usando a tecnologia NetApp FlexClone

  É necessária uma licença FlexClone no sistema de storage onde você deseja criar o clone.

- Suporte para o recurso instantâneo do grupo de consistência (CG) do ONTAP como parte da criação de backups.
- Funcionalidade de executar vários backups simultaneamente em vários hosts de recursos

  Em uma única operação, os snapshots são consolidados quando os recursos em um único host compartilham o mesmo volume.

- Capacidade de criar instantâneos usando comandos externos.
- Suporte para Linux LVM no sistema de arquivos XFS.

Tipos de armazenamento suportados pelo plug-in SnapCenter para PostgreSQL

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e máquinas virtuais (VMs). Você deve verificar o suporte para o seu tipo de armazenamento antes de instalar o plug-in SnapCenter para PostgreSQL.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados a FC • LUNs ligados ao iSCSI • Volumes conectados a NFS

Máquina	Tipo de armazenamento
VMware ESXi	• LUNs RDM conetados por um FC ou iSCSI ESXi HAScanning de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluído 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** para 1 para reexaminar somente os HBA listados em HBA_DRIVER_NAMES. • ISCSI LUNs ligados 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 da VVol em NFS e SAN O armazenamento de dados da VVol só pode ser provisionado com as Ferramentas do ONTAP para o VMware vSphere.

Mínimo de ONTAP Privileges necessário para o plug-in PostgreSQL

Os ONTAP Privileges mínimos necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
  - event generate-AutoSupport-log
  - mostra o histórico de trabalhos
  - paragem do trabalho
  - lun
  - lun criar
  - lun criar
  - lun criar
  - eliminação lun
  - lun igrop add
  - lun igrop criar

- eliminação do agrupamento lun
- mudar o nome do grupo lun
- mudar o nome do grupo lun
- show de grupos de lun
- nós complementares de mapeamento de lun
- mapeamento lun criar
- eliminação do mapeamento lun
- mapeamento lun remove-reporting-nonos
- mostra de mapeamento lun
- modificação de lun
- movimentação de lun no volume
- lun offline
- lun online
- limpeza da reserva persistente de lun
- redimensionar lun
- série lun
- mostra lun
- regra adicional de política do SnapMirror
- regra de modificação de política do SnapMirror
- regra de remoção da política do SnapMirror
- SnapMirror policy show
- restauração de SnapMirror
- SnapMirror show
- SnapMirror show-history
- atualização do SnapMirror
- SnapMirror update-ls-set
- SnapMirror lista-destinos
- versão
- clone de volume criar
- show de clone de volume
- início da divisão do clone de volume
- paragem dividida clone volume
- criar volume
- destruição de volume
- clone de arquivo de volume criar
- show-disk-use do arquivo de volume
- volume off-line

    - volume online
    - modificação do volume
    - criar qtree de volume
    - eliminação de qtree de volume
    - modificação de qtree de volume
    - apresentação de qtree de volume
    - restrição de volume
    - apresentação do volume
    - criar instantâneo de volume
    - eliminar instantâneo do volume
    - modificação do instantâneo do volume
    - tempo de expiração do volume snapshot modify-SnapLock
    - mudar o nome do instantâneo do volume
    - restauração de snapshot de volume
    - restauração de arquivo de snapshot de volume
    - apresentação de instantâneo do volume
    - desmontar o volume
    - svm cifs
    - compartilhamento cifs de svm criar
    - exclusão de compartilhamento cifs de svm
    - apresentação do shadowcopy cifs de svm
    - exibição de compartilhamento cifs de svm
    - mostra cifs de svm
    - política de exportação de svm
    - criação de política de exportação de svm
    - exclusão da política de exportação do svm
    - regra de política de exportação de svm criar
    - a regra de política de exportação do svm é exibida
    - exibição da política de exportação do svm
    - svm iscsi
    - apresentação da ligação iscsi de svm
    - mostra o svm
- Comandos somente leitura: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
    - interface de rede
    - mostra da interface de rede
    - svm

Prepare sistemas de storage para replicação SnapMirror e SnapVault para PostgreSQL

Você pode usar um plug-in do 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 disco a disco para conformidade com os padrões e outros fins relacionados à governança. Antes de executar essas tarefas, você deve configurar uma relação de proteção de dados entre os volumes de origem e destino e inicializar a relação.

O SnapCenter executa as atualizações para o SnapMirror e o SnapVault após concluir a operação de captura instantânea. As atualizações SnapMirror e SnapVault são executadas como parte da tarefa SnapCenter; não crie uma agenda ONTAP separada.

Se você estiver vindo para o SnapCenter de um produto NetApp SnapManager e estiver satisfeito com as relações de proteção de dados que configurou, ignore esta seção.

Uma relação de proteção de dados replica dados no storage primário (o volume de origem) para o storage secundário (o volume de destino). Ao inicializar a relação, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não suporta relações em cascata entre volumes SnapMirror e SnapVault (**Primary** > **Mirror** > **Vault**). Você deve usar relacionamentos de fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis de versão e como configurá-los, consulte "Documentação do ONTAP".

Estratégia de backup para PostgreSQL

Defina uma estratégia de backup para PostgreSQL

Definir uma estratégia de backup antes de criar seus trabalhos de backup ajuda a ter os backups necessários para restaurar ou clonar seus recursos com êxito. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (rto) e objetivo do ponto de restauração (RPO) determinam em grande parte a sua estratégia de backup.

Sobre esta tarefa

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. Rto é o momento em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a era dos arquivos que precisam 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 de seus recursos.
2. Decida quantos trabalhos de cópia de segurança necessita.
3. Decida como nomear seus backups.
4. Decida se deseja criar uma política baseada em cópia Snapshot para fazer backup de snapshots

consistentes com aplicações do cluster.

5. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção a longo prazo.
6. Determine o período de retenção dos snapshots no sistema de storage de origem e no destino do SnapMirror.
7. Determine se deseja executar quaisquer comandos antes ou depois da operação de backup e forneça um prescritor ou postscript.

Descoberta automática de recursos no host Linux

Os recursos são clusters e instâncias do PostgreSQL no host Linux que são gerenciados pelo SnapCenter. Depois de instalar o plug-in do SnapCenter para PostgreSQL, os clusters do PostgreSQL de todas as instâncias desse host são automaticamente descobertos e exibidos na página recursos.

Tipos de backups suportados

Tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter é compatível com o tipo de backup baseado em cópia de snapshot para clusters PostgreSQL.

Backup baseado em cópia snapshot

Os backups baseados em cópias snapshot utilizam a tecnologia NetApp snapshot para criar cópias on-line e somente leitura dos volumes nos quais os clusters PostgreSQL residem.

Como o plug-in do SnapCenter para PostgreSQL usa snapshots de grupo de consistência

Você pode usar o plug-in para criar snapshots de grupo de consistência para grupos de recursos. Um grupo de consistência é um contentor que pode abrigar vários volumes para que você possa gerenciá-los como uma entidade. Um grupo de consistência são snapshots 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 **descontraído**. Você também pode ativar ou desativar a sincronização WAFL (Write Anywhere File Layout) durante uma operação consistente de snapshot em grupo. O WAFL Sync melhora o desempenho de um snapshot de grupo de consistência.

Como o SnapCenter gerencia o gerenciamento de backups de dados

O SnapCenter gerencia o gerenciamento de backups de dados nos níveis do sistema de storage e do sistema de arquivos.

Os instantâneos no armazenamento primário ou secundário e suas entradas correspondentes no catálogo PostgreSQL são excluídos com base nas configurações de retenção.

Considerações para determinar agendas de backup para PostgreSQL

O fator mais crítico na determinação de um agendamento de backup é a taxa de alteração do recurso. Você pode fazer backup de um recurso muito usado a cada hora, enquanto você pode fazer backup de um recurso raramente usado uma vez por dia. Outros fatores incluem a importância do recurso para a sua organização, seu contrato de nível de serviço (SLA) e seu objetivo do ponto de restauração (RPO).

Os programas de backup têm duas partes, como segue:

- Frequência de backup (com que frequência os backups devem ser executados)

  A frequência de backup, também chamada de tipo de programação para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como hora, dia, semanal ou mensal.

- Programações de backup (exatamente quando os backups devem ser executados)

  As agendas de backup fazem parte de uma configuração de recurso ou grupo de recursos. Por exemplo, se você tiver um grupo de recursos que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas

Número de trabalhos de backup necessários para PostgreSQL

Os fatores que determinam o número de tarefas de backup de que você precisa 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 Plug-in para PostgreSQL

Você pode usar a convenção padrão de nomenclatura Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um carimbo de data/hora aos nomes de Snapshot 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 carimbo de data/hora.

Como alternativa, você pode especificar o formato do nome da captura Instantânea enquanto protege recursos ou grupos de recursos selecionando **usar formato de nome personalizado para cópia Instantânea**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por padrão, o sufixo do carimbo de hora é adicionado ao nome do instantâneo.

Estratégia de restauração e recuperação para PostgreSQL

Defina uma estratégia de restauração e recuperação para os recursos PostgreSQL

Você deve definir uma estratégia antes de restaurar e recuperar o cluster para que possa executar operações de restauração e recuperação com sucesso.

Somente a recuperação manual do cluster é suportada.

Passos

1. Determine as estratégias de restauração suportadas para recursos PostgreSQL adicionados manualmente
2. Determine 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 executar operações de restauração com êxito usando o SnapCenter.

Você não pode recuperar recursos 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 obtidos após o snapshot selecionado para restauração em tais 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 uma pasta backup_label e tablespace_map na pasta */<OS_temp_folder>/postgresql_SC_recovery*<Restore_JobId>/_ para ajudar a recuperar manualmente .

Tipo de estratégia de restauração suportada para PostgreSQL descoberto automaticamente

Você deve definir uma estratégia antes de executar operações de restauração com êxito usando o SnapCenter.

A restauração completa de recursos é a estratégia de restauração suportada para 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 do SnapCenter para PostgreSQL é compatível com SnapRestore de arquivo

único e tipos de restauração de conexão e cópia para clusters PostgreSQL descobertos automaticamente.

O SnapRestore de arquivo único é executado em ambientes NFS para os seguintes cenários:

- Se apenas a opção **Complete Resource** estiver selecionada
- Quando o backup selecionado é de um local secundário SnapMirror ou SnapVault e a opção **recurso completo** está selecionada

O SnapRestore de Arquivo único é executado em ambientes SAN para os seguintes cenários:

- Se apenas a opção **Complete Resource** estiver selecionada
- Quando o backup é selecionado em um local secundário do SnapMirror ou do SnapVault e a opção **recurso completo** está selecionada

Tipos de operações de recuperação compatíveis com clusters PostgreSQL

O SnapCenter permite que você execute diferentes tipos de operações de recuperação para clusters PostgreSQL.

- Recupere o cluster até o estado mais recente
- Recupere o cluster até um ponto específico no tempo

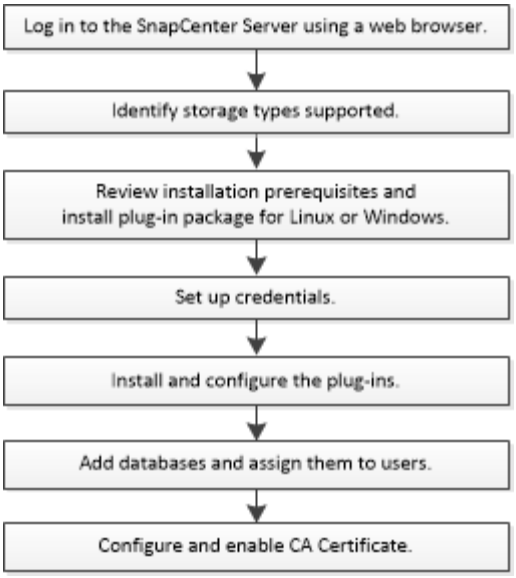
  Você deve especificar a data e a hora para a recuperação.

O SnapCenter também fornece 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 plug-in do SnapCenter para PostgreSQL se quiser proteger clusters do 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 completar todos os requisitos. O plug-in SnapCenter para PostgreSQL está disponível em ambientes Windows e Linux.

- Você deve ter instalado o Java 11 em seu host.

  O IBM Java não é suportado.

- Para 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 do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host. O plug-in SnapCenter para Microsoft Windows será implantado por padrão com o plug-in PostgreSQL em hosts Windows.
- O servidor SnapCenter deve ter acesso ao 8145 ou à porta personalizada do plug-in para o host PostgreSQL.

Hosts do Windows

- Você deve ter um usuário de domínio com Privileges de administrador local com permissões de login local no host remoto.
- Ao instalar o plug-in para PostgreSQL em um host Windows, o plug-in SnapCenter 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 em seu host Windows.

  "Downloads Java para todos os sistemas operacionais"

  "Ferramenta de Matriz de interoperabilidade do 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 em seu host Linux.

  "Downloads Java para todos os sistemas operacionais"

  "Ferramenta de Matriz de interoperabilidade do NetApp"

- Para clusters PostgreSQL que estão sendo executados em um host Linux, ao instalar o plug-in para PostgreSQL, o plug-in SnapCenter para UNIX é instalado automaticamente.
- Você deve ter **bash** como o shell padrão para instalação do plug-in.

Comandos suplementares

Para executar um comando complementar no plug-in do SnapCenter para PostgreSQL, você deve incluí-lo no arquivo *allowed_commands.config*.

- Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
- Localização 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 são sensíveis a maiúsculas e minúsculas. Certifique-se de especificar o nome de caminho totalmente qualificado e incluir o nome de caminho entre aspas (") se ele contiver espaços.

Por exemplo:

Comando: Comando de montagem: Comando umount: Comando "C: Arquivos de programas/NetApp comandos do SnapCreator" comando: myscript.bat

Se o arquivo *allowed_commands.config* não estiver presente, os comandos ou a execução de 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.

Configure sudo Privileges 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 de plug-in serão executados como um usuário não-root eficaz. Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se o umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro devem ter permissão de 555. Caso contrário, a instalação do plug-in pode falhar.
- Para o usuário não-root, certifique-se de que o nome do usuário não-root e do grupo do usuário devem ser os mesmos.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos de código de autenticação de mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

  Reinicie o serviço sshd depois de 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 o sudo Privileges para que o usuário não-root forneça acesso aos seguintes caminhos:

- /Home/*Linux_USER*/.SC_NetApp/SnapCenter_linux_host_plugin.bin
- /Custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/SnapCenter/spl/bin/spl

Passos

1. Faça 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 !visiblepw
Defaults: LINUX_USER !requiretty
```

Se você estiver tendo uma configuração RAC, juntamente 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**, que está localizado em:

- _C: /ProgramData/NetApp/SnapCenter/Repositório de pacotes/sc_unix_plugins_checksum.txt _ se o servidor SnapCenter estiver instalado no host do Windows.
- _/opt/NetApp/SnapCenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ se o servidor SnapCenter 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 do 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 do sistema host e requisitos de dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• DOTNET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell Core 7.4.2 Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet."

Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux

Antes de instalar o pacote de plug-ins do 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 • SUSE Linux Enterprise Server (SLES) Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto. Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Configure 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 raiz ou para um usuário não-root que tenha sudo Privileges para instalar e iniciar o processo de plug-in.

Prática recomendada: embora você tenha permissão para criar credenciais para Linux após implantar hosts e instalar plug-ins, a prática recomendada é criar credenciais após adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

  Você deve configurar as credenciais do Windows antes de instalar os plug-ins.

  Você deve configurar as credenciais com o Privileges 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 Privileges de administrador completo, será necessário atribuir pelo menos o grupo de recursos e Privileges de backup ao nome de usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Clique em **novo**.
4. Na página Credential (credencial), especifique as informações necessárias para configurar credenciais:

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para as credenciais.

Para este campo…	Faça isso…
Nome de utilizador	Introduza o nome de utilizador e a palavra-passe a utilizar para a 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 no qual você está instalando o plug-in do SnapCenter. Formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS_username* ◦ *Domain FQDN_username* • Administrador local (apenas para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é: *Nome de usuário* Não use aspas duplas (") ou backtick (') nas senhas. Você não deve usar os símbolos menos de (>) e exclamação (!) juntos em senhas. Por exemplo, lessthan!10, lessthan10You!, backtick'12.
Palavra-passe	Introduza a palavra-passe utilizada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que pretende utilizar.
Use sudo Privileges	Marque a caixa de seleção **Use sudo Privileges** se estiver criando credenciais para um usuário que não seja root. Aplicável apenas a usuários 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.

Configure o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite criar uma conta de serviço gerenciado de grupo (gMSA) que fornece gerenciamento automatizado de senha de conta de serviço a partir de uma conta de domínio gerenciado.

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 é um membro do domínio.

Passos

1. Crie uma chave raiz KDS para gerar senhas exclusivas para cada objeto em seu gMSA.
2. Para cada domínio, execute o seguinte comando do 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,…>
.. Execute `Get-ADServiceAccount` o comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:
   a. Ative o módulo do ative Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando do 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 o host.

b. Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua o Privileges administrativo ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no servidor SnapCenter.

   O servidor SnapCenter 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.

Instale o plug-in SnapCenter para PostgreSQL

Adicione hosts e instale pacotes plug-in 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 servidor SnapCenter for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deve executar o seguinte:
  - Atualize para o Windows Server 2019 (versão de SO 17763,5936) ou posterior
  - Atualize para o Windows Server 2022 (versão de SO 20348,2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está

integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar 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 você estiver usando a conta de serviço gerenciado de grupo (gMSA), você deve configurar o gMSA com Privileges administrativo.

  "Configurar conta de serviço gerenciado de grupo no Windows Server 2016 ou posterior para PostgreSQL"

Sobre esta tarefa

- Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Verifique se a guia **hosts gerenciados** está selecionada na parte superior.
3. Clique em **Add**.
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 cliente PostgreSQL, e este host pode estar em um sistema Windows ou em um sistema Linux.
Nome do host	Insira o nome do host de comunicação. Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no 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 exibir detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você forneceu. 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 instalar.

   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	Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido 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, você deve especificar a mesma porta. Caso contrário, a operação falha.
Caminho de instalação	O Plug-in para PostgreSQL é instalado no host cliente PostgreSQL, e este host pode estar em um sistema Windows ou em um sistema Linux. • Para o pacote de plug-ins do 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 do SnapCenter para Linux, o caminho padrão é /opt/NetApp/SnapCenter. Opcionalmente, você pode personalizar o caminho.

Para este campo…	Faça isso…
Ignorar as verificações de pré-instalação	Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.
Adicione todos os hosts no cluster	Marque esta caixa de seleção para adicionar todos os nós de cluster.
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	Para o host Windows, marque essa caixa de seleção se desejar usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in. Forneça o nome do gMSA no seguinte formato: O gMSA será usado como uma conta de serviço de logon apenas para o serviço SnapCenter Plug-in para Windows.

7. Clique em **Enviar**.

   Se você não tiver selecionado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se o host 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 Java (para plug-ins do Linux) são validados de acordo com os requisitos mínimos. Se os requisitos mínimos não forem cumpridos, são apresentadas mensagens de erro ou de aviso adequadas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado no NetApp SnapCenter para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, será necessário atualizar o arquivo em ambos os nós.

8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirm and Submit**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós no cluster.

   A verificação de impressões digitais é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitorize o progresso da instalação.
   - Para o plug-in do Windows, os logs de instalação e atualização estão localizados em: *C: Plug-in do Windows SnapCenter*<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_

Instale pacotes de plug-ins do 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 PowerShell.

Antes de começar

Você deve ter feito 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 servidor SnapCenter, 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*. Em alternativa, pode também consultar o "Guia de referência de 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 SnapCenter Plug-in para cluster PostgreSQL usando a interface de usuário (UI) do SnapCenter. Se o seu ambiente não permitir a instalação remota do plug-in a partir da IU do SnapCenter, você pode instalar o plug-in para cluster PostgreSQL no modo 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 um dos hosts Linux onde o cliente PostgreSQL reside.
- O host Linux no qual você está instalando o SnapCenter Plug-in para 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 do NetApp"

- O cluster do SnapCenter Plug-in para PostgreSQL faz parte do pacote de plug-ins do SnapCenter para Linux. Antes de instalar o pacote de plug-ins do SnapCenter para Linux, você já deve ter instalado o SnapCenter em um host do Windows.

Passos

1. Copie o pacote de plug-ins do SnapCenter SnapCenter para o arquivo de instalação do Linux

(SnapCenter_linux_host_plugin.bin) do NetApp para o host onde você deseja instalar o plug-in para o PostgreSQL.

Você pode acessar esse caminho a partir do host onde o servidor SnapCenter 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 SMCore.
   - -DSERVER_IP especifica o endereço IP do servidor SnapCenter.
   - -DSERVER_HTTPS_PORT especifica a porta HTTPS do servidor SnapCenter.
   - -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 /<installation directory>/NetApp/SnapCenter/scc/etc/SC_SMS_Services.properties e, em seguida, adicione o parâmetro PLUGINS_ENABLED: PostgreSQL:3,0.
5. Adicione o host ao servidor SnapCenter 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Monitore o status da instalação do Plug-in para PostgreSQL

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
   a. Clique em **filtro**.
   b. Opcional: Especifique a data de início e fim.
   c. No menu suspenso tipo, selecione **Instalação 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 **Visualizar logs**.

Configurar certificado CA

Gerar arquivo CSR do 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 a CSR gerada. O certificado terá uma chave privada associada a ele.

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

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

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

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

Para configurações de cluster, o nome do cluster (FQDN de cluster virtual) e os respetivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome alternativo (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados CA

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.

4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 **Yes**, importe a chave privada e clique em **Next**.
Importar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

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

7. Repita o passo 5 para a pasta "Pessoal".

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia 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 **thumbprint**.
   d. Copie os carateres 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

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.

Configure o certificado CA com os serviços de plug-in do host do Windows

Você deve configurar o certificado CA com os serviços de plug-in host do Windows para ativar o certificado digital instalado.

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, 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"
   ```

Configure o certificado CA para o serviço de plug-ins SnapCenter PostgreSQL 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. Altere a senha do keystore:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Altere a senha para 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 depois de 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. Liste 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 de CA raiz e, em seguida, os certificados de CA intermediários.

Configurar o par de chaves assinadas pela CA para plug-in de armazenamento confiável

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. Liste 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. Liste os certificados adicionados no keystore.

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

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

   A senha padrão do keystore 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 espaço ou
   carateres 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 com a chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o plug-in trust-store.

Configurar a lista de revogação de certificados (CRL) para plug-ins do SnapCenter

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 SnapCenter é 'opt/NetApp/snapcenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties contra a chave CRL_PATH.

   Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Configure o certificado CA para o serviço de plug-ins PostgreSQL do SnapCenter 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 Plug-ins 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. Altere 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 por seu caminho completo.

   C: Arquivos de programas/<jdk_version>/keytool.exe" -storepasswd -keystore keystore.jks

3. Altere a senha para 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*.

4. Reinicie o serviço depois de 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. Liste 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 de CA raiz e, em seguida, os certificados de CA intermediários.

Configurar o par de chaves assinadas pela CA para plug-in de armazenamento confiável

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. Liste 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 -destinkeystore keystore.jks -deststoretype JKS

5. Liste os certificados adicionados no keystore.

   keytool -list -v -keystore keystore.jks

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da 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

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

   Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o plug-in trust-store.

Configurar a lista de revogação de certificados (CRL) para plug-ins do SnapCenter

Sobre esta tarefa

- Para transferir o ficheiro CRL mais recente para o certificado CA relacionado, "Como atualizar o arquivo

de lista de revogação de certificados no certificado da CA do SnapCenter"consulte .

- 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* contra a chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

   Os certificados recebidos serão verificados em relação a cada CRL.

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet RUN *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando as *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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- * * Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da 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 são concluídas com êxito.

Preparar-se para a proteção de dados

Pré-requisitos para usar o plug-in SnapCenter para PostgreSQL

Antes de usar o plug-in do SnapCenter para PostgreSQL, o administrador do SnapCenter deve instalar e configurar o servidor SnapCenter e executar as tarefas de pré-requisito.

- Instalar e configurar o servidor SnapCenter.
- Inicie sessão no servidor SnapCenter.
- Configure o ambiente SnapCenter adicionando conexões do sistema de storage e criando credenciais, se aplicável.
- Instale o Java 11 em seu host Linux ou Windows.

  Você deve definir o caminho Java na variável caminho ambiental da máquina host.

- Configure o SnapMirror e o SnapVault, se quiser replicação de backup.

Como recursos, grupos de recursos e políticas são usados para proteger o PostgreSQL

Antes de usar o SnapCenter, é útil entender 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 que você faz backup ou clonar com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host.

  Quando você executa uma operação em um grupo de recursos, executa essa operação nos recursos definidos no grupo de recursos de acordo com a programação especificada 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 programados para recursos únicos e grupos de recursos.

- As políticas especificam a frequência do backup, a replicação, os scripts e outras caraterísticas 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 quando você executa um backup sob demanda para um único recurso.

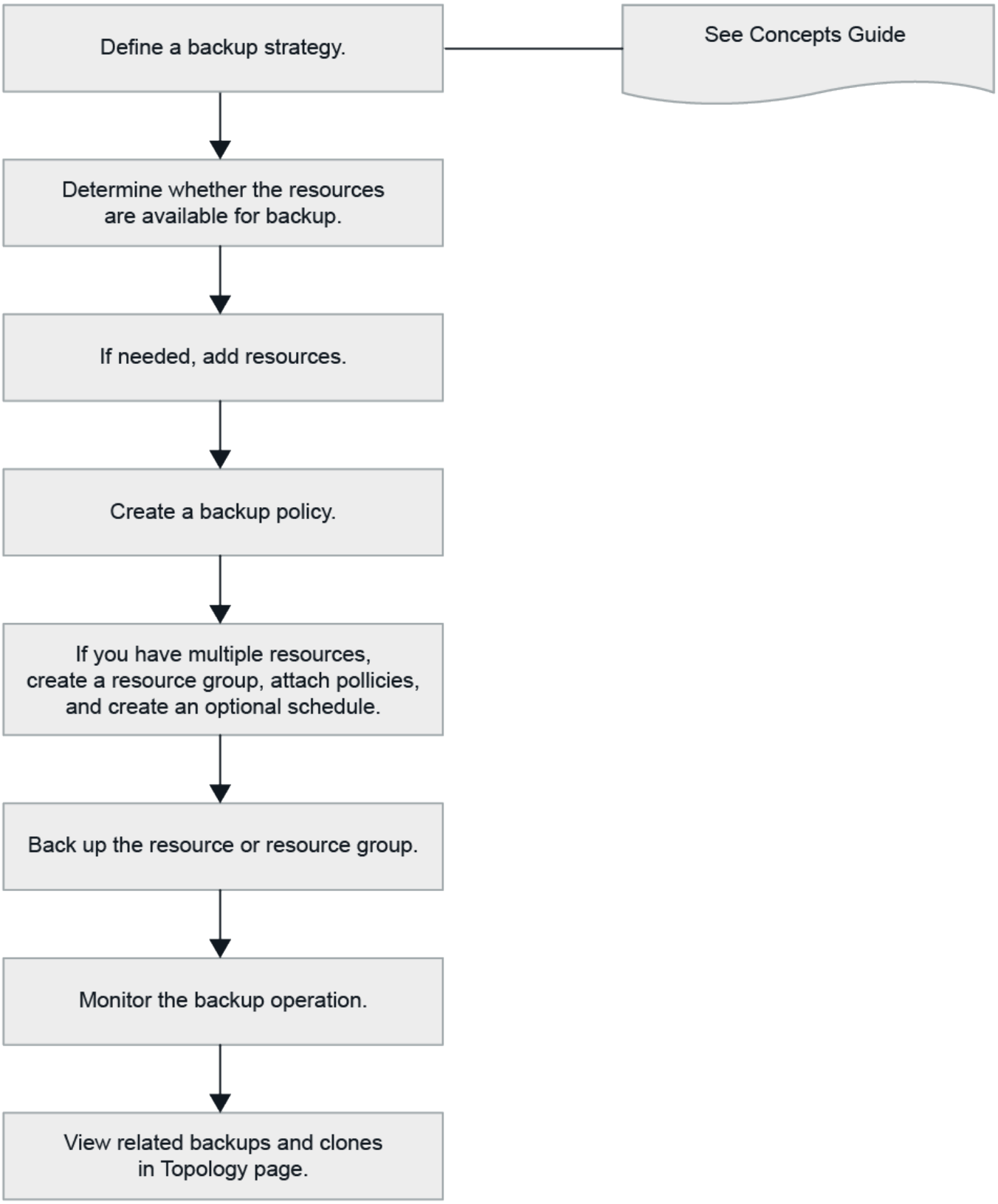
Pense em um grupo de recursos como definindo o que você quer proteger e quando você quer protegê-lo em termos de dia e tempo. Pense em uma política como definir como você deseja protegê-la. Se você estiver fazendo backup de todos os clusters, por exemplo, poderá criar um grupo de recursos que inclua todos os clusters no host. Em seguida, você pode anexar duas políticas ao grupo de recursos: Uma política diária e uma política por hora. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diariamente.

Faça backup dos recursos do PostgreSQL

Faça 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 dos clusters para backup, gerenciamento de políticas de backup, criação de grupos de recursos e inclusão 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 clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell. "Guia de referência de cmdlet do software SnapCenter".

Descobrir os clusters automaticamente

Os recursos são clusters PostgreSQL no host Linux que são gerenciados pelo SnapCenter. Você pode adicionar os recursos a grupos de recursos para executar operações de proteção de dados depois de descobrir os clusters do PostgreSQL disponíveis.

Antes de começar

- Você já deve ter concluído tarefas como instalar o servidor SnapCenter, adicionar hosts e configurar as conexões do sistema de armazenamento.
- O plug-in do SnapCenter para PostgreSQL não oferece suporte à descoberta automática dos recursos residentes em ambientes virtuais RDM/VMDK.

Sobre esta tarefa

- Depois de instalar o plug-in, todos os clusters nesse host Linux são automaticamente descobertos e exibidos na página recursos.
- Somente clusters são auto-descobertos.

Os recursos descobertos automaticamente não podem ser modificados ou excluídos.

Passos

1. No painel de navegação à esquerda, clique em **Resources** 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 selecione o nome do host.

   Em seguida, pode clicar em* * para fechar o painel do filtro.

4. Clique em **Atualizar recursos** para descobrir os recursos disponíveis no host.

   Os recursos são exibidos juntamente 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, então não protegido será exibido na coluna Estado geral.
   - Se o cluster estiver em um sistema de armazenamento NetApp e protegido, e se não houver operação de backup executada, o Backup não executado será exibido na coluna Status geral. O status mudará para Backup failed ou Backup successful com base no último status de backup.

É necessário atualizar os recursos se os clusters forem renomeados fora do SnapCenter.

Adicione recursos manualmente ao host do plug-in

A deteção 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 servidor SnapCenter, adicionar hosts e configurar conexões do sistema de armazenamento.

Sobre esta tarefa

A deteção automática não é suportada para as seguintes configurações:

- Layouts RDM e VMDK

Passos

1. No painel de navegação à esquerda, selecione o plug-in do SnapCenter para PostgreSQL na lista suspensa e clique em **recursos**.
2. Na página recursos, clique em **Adicionar recursos 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	Insira o nome do host.
Tipo	Selecione cluster.
Instância	Especifique o nome da instância, que é o pai do cluster.
Credenciais	Selecione as credenciais ou adicione informações para a credencial. Isso é opcional.

4. Na página fornecer espaço físico 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 valor de chave personalizados para o plug-in PostgreSQL
6. Revise o resumo e clique em **Finish**.

   Os clusters são exibidos juntamente com informações como o nome do host, grupos e políticas de recursos associados e status geral

Se você quiser fornecer aos usuários acesso a recursos, você deve atribuir os recursos aos usuários. Isso permite que os usuários executem as ações para as quais eles têm permissões nos ativos que são atribuídos a eles.

"Adicione um usuário ou grupo e atribua funções e ativos"

Depois de 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.

- Quando você modifica os recursos adicionados manualmente que são migrados do SnapCenter 5,0 ou anterior, faça o seguinte na página **Configurações de recurso** para pares de valores de chave personalizados:
  - Especifique o termo "PORT" no campo **Name**.
  - Especifique o número da porta no campo **valor**.

Crie políticas de backup para PostgreSQL

Antes de usar o SnapCenter para fazer backup dos recursos do PostgreSQL, você deve criar uma política de backup para o grupo de recursos ou recursos que deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e retém backups.

Antes de começar

- Você precisa 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 precisa se preparar para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, configurar conexões do sistema de storage e adicionar recursos.
- O administrador do SnapCenter deve ter atribuído os SVMs para os volumes de origem e destino a você se estiver replicando snapshots em um espelho ou cofre.

  Além disso, você pode especificar as 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 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio de instantâneos impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na política.
  - Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

> As configurações do SnapLock primário são gerenciadas na política de backup do SnapCenter e as configurações do SnapLock secundário são gerenciadas pelo ONTAP.

Passos

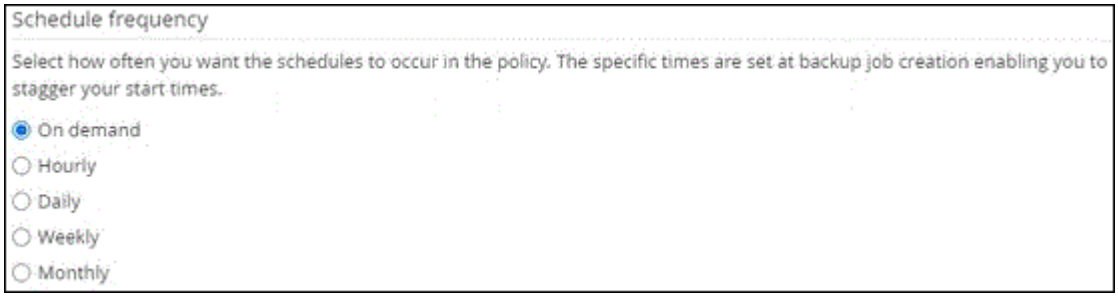
1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **políticas**.
3. Clique em **novo**.
4. Na página Nome, insira o nome e a descrição da política.

5. Na página tipo de política, execute o seguinte:
   a. Selecione o tipo de armazenamento.
   b. Na seção **Configurações personalizadas de backup**, forneça quaisquer configurações específicas de backup que tenham que ser passadas para o formato de valor de chave do plug-in.

      Você pode fornecer vários valores-chave a serem passados para o plug-in.

6. Na página Snapshot, especifique o tipo de agendamento selecionando **On Demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.

   Você pode especificar a programação (data de início, data de término e frequência) para a operação de backup enquanto cria 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 programações de backup a cada política.



   Se você tiver agendado para as 2:00 da manhã, o horário não será acionado durante o horário de verão (DST).

7. Na seção Configurações de instantâneos, especifique o número de instantâneos que você deseja manter.
8. Na página retenção, 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 instantâneos	Selecione **Copies to keep** e especifique o número de instantâneos que deseja manter. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro.

   Para backups baseados em cópias Snapshot, defina a contagem de retenção para 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção pode falhar porque o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino.

9. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas

Um grupo de recursos é o contentor ao qual você deve adicionar recursos que deseja fazer backup e proteger. Um grupo de recursos permite fazer 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 tarefa de proteção de dados que deseja executar.

Sobre esta tarefa

- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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	Introduza um nome para o grupo de recursos. O nome do grupo de recursos não deve exceder 250 carateres.
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.
Use o formato de nome personalizado para cópia instantânea	Marque essa 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 carimbo de data/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 **Resource Type**.

   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**.

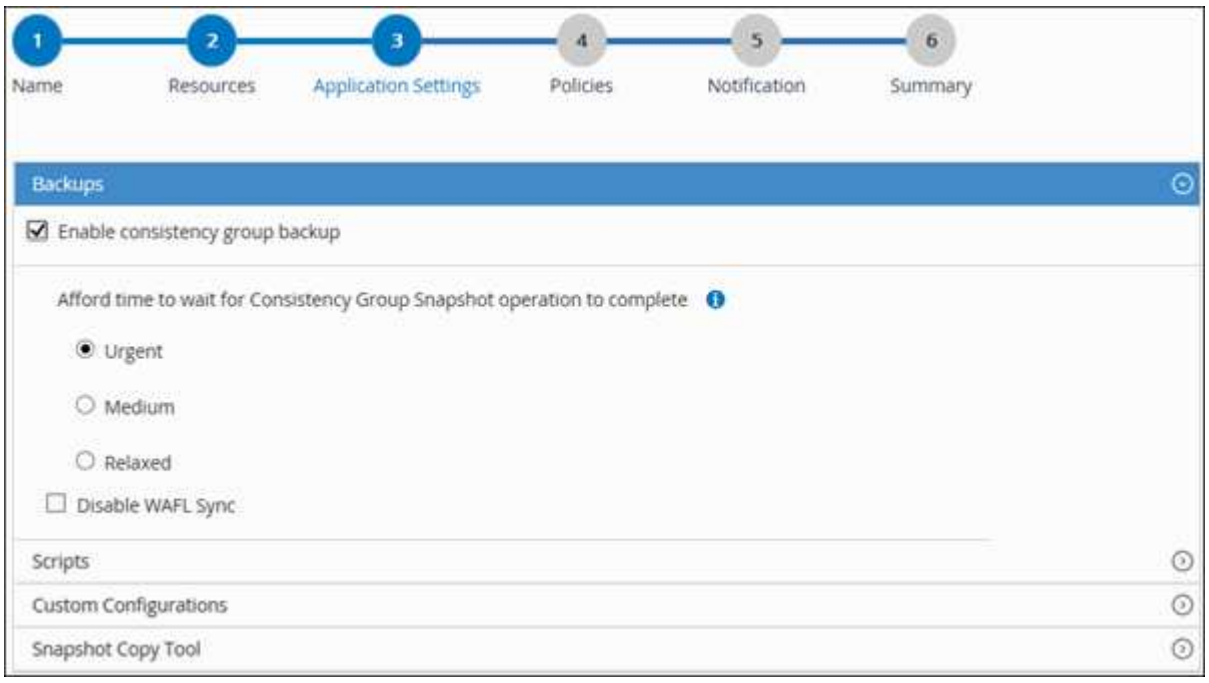
6. Na página Configurações do aplicativo, faça o seguinte:

   a. Clique na seta **backups** para definir opções adicionais de backup:

      Ative o backup do grupo de consistência e execute as seguintes tarefas:

Para este campo…	Faça isso…
Tenha tempo para esperar que a operação de snapshot do Grupo de consistência seja concluída	Selecione **urgente**, **Médio** ou **relaxado** para especificar o tempo de espera para que a operação de snapshot seja concluída. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a 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 quiesce, snapshot e unquiesce. Também pode introduzir os pré comandos a serem executados antes de sair em caso de falha.

   b. Clique na seta **Custom Configurations** (Configurações personalizadas) e insira os pares de valor de chave personalizados necessários para todas as operações de proteção de dados usando esse recurso.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_ENABLE	(Y/N)	Permite que a gestão do registo de arquivo elimine os registos de arquivo.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_RETENÇÃO	number_of_days	Especifica o número de dias em que os logs de arquivo são mantidos. Esta definição tem de ser igual ou superior a NTAP_SNAPSHOT_ RETENÇÕES.
ARCHIVE_LOG_DIR	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs do arquivo.
ARCHIVE_LOG_EXT	extensão_ficheiro	Especifica o comprimento da extensão do arquivo de log do arquivo. Por exemplo, se o log de arquivo 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.
ARCH ARCHIVE_LOG_RECURSIVE_ SE	(Y/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs do arquivo estiverem localizados em subdiretórios.

Os pares de chave-valor personalizados são suportados para sistemas de plug-in PostgreSQL Linux e não são suportados para cluster PostgreSQL registrado como um plug-in centralizado do Windows.

c. Clique na seta **Snapshot Copy Tool** 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, essa opção não é aplicável.	Selecione **SnapCenter com consistência do sistema de arquivos**.
SnapCenter para criar um instantâneo de nível de storage	Selecione **SnapCenter sem consistência do sistema de arquivos**.

Se você quiser…	Então…
Para inserir o comando a ser executado no host para criar cópias snapshot.	Selecione **Other** e, em seguida, digite 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 programações para políticas selecionadas.

   b. Na coluna Configurar agendas, clique em + para a política que deseja configurar.

   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e clique em **OK**.

      Onde, policy_name é o nome da política selecionada.

      As programações configuradas são listadas na coluna **programações aplicadas**.

   As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas 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 **Finish**.

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 Administrador da infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estão em andamento.

  As instalações de plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento, pois 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 do sistema de armazenamento devem ser exclusivos.

  O SnapCenter não é compatível com vários sistemas de storage com o mesmo nome em clusters diferentes. Cada sistema de storage com suporte do SnapCenter deve ter um nome exclusivo e um endereço IP de 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 servidor SnapCenter.

```
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:

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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Faça backup do PostgreSQL

Se um recurso ainda não fizer parte de qualquer 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 uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.
- Para a operação de backup baseada em cópia Snapshot, verifique se todos os clusters de locatários estão válidos e ativos.
- Para comandos pré e POST para operações quiesce, Snapshot e unquiesce, você deve verificar se os comandos existem na lista de comandos disponível no host plug-in dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização padrão no host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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, em seguida, selecione o nome do host e o tipo de recurso para filtrar os recursos. Em seguida, pode selecionar para fechar o painel de filtro.
3. Selecione o recurso que você deseja fazer backup.
4. Na página recurso, selecione **Use o formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.
5. Na página Configurações do aplicativo, faça o seguinte:
   - Selecione a seta **backups** para definir opções adicionais de backup:

     Ative o backup do grupo de consistência, se necessário, e execute as seguintes tarefas:

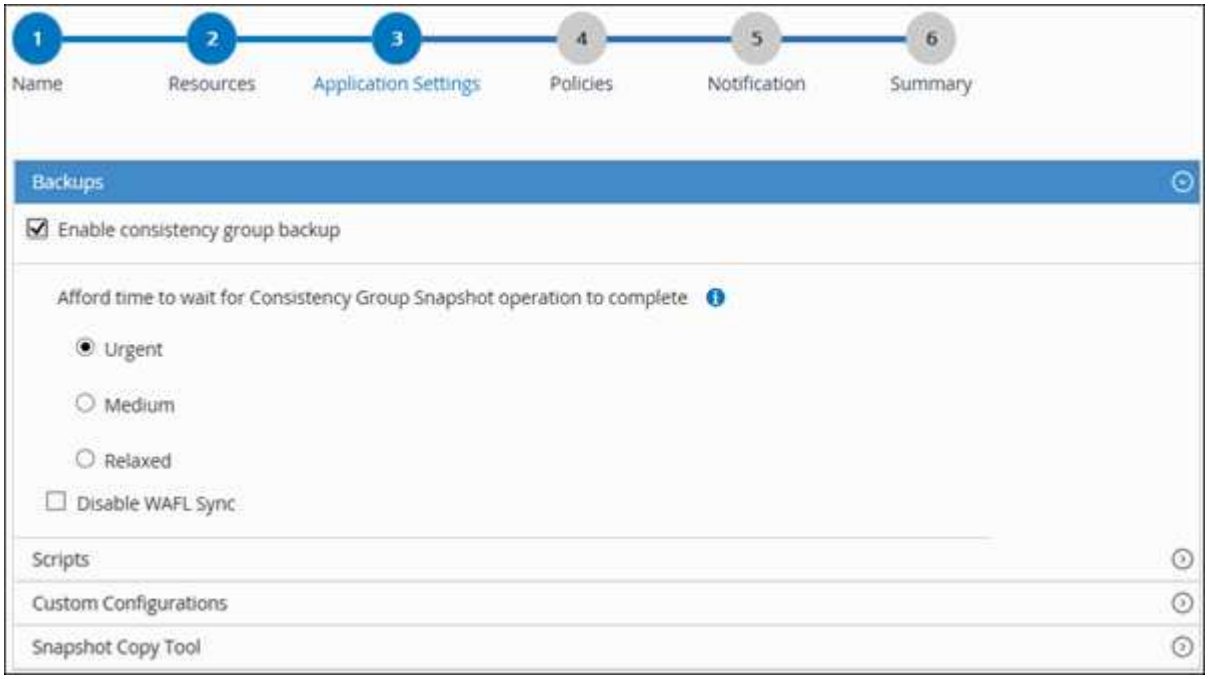
Para este campo…	Faça isso…
Tenha tempo para esperar a conclusão da operação "Consistency Group Snapshot"	Selecione **urgente**, **Médio** ou **relaxado** para especificar o tempo de espera para que a operação Snapshot termine. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL.

   - Selecione a seta **Scripts** para executar comandos pré e POST para operações quiesce, Snapshot e unquiesce.

     Você também pode executar pré-comandos antes de sair da operação de backup. Os Prescripts e postscripts são executados no servidor SnapCenter.
   - Selecione a seta **Custom Configurations (Configurações personalizadas) e, em seguida, insira os pares de valores personalizados necessários para todos os trabalhos que usam esse recurso.
   - Selecione a seta **Snapshot Copy Tool** para selecionar a ferramenta para criar instantâneos:

Se você quiser…	Então…
SnapCenter para criar um Snapshot no nível de storage	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 instantâneo	Selecione **SnapCenter com consistência do sistema de arquivos**.
Para inserir o comando para criar uma captura Instantânea	Selecione **Other** e, em seguida, digite o comando para criar uma captura Instantânea.



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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Selecione + * * na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e selecione **OK**.

      policy_name é o nome da política selecionada.

   As programações configuradas são listadas na coluna agendas aplicadas.

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 **Finish**.

   A página de topologia de recursos é exibida.

9. Selecione **fazer uma cópia de segurança 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. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.
    - Nas configurações do MetroCluster, o SnapCenter pode não ser capaz de detetar uma relação de proteção após um failover.

      Para obter informações, consulte: "Não é possível detetar a relação SnapMirror ou SnapVault após o failover do MetroCluster"

    - Se você estiver fazendo backup de dados de aplicativos em VMDKs e o tamanho de heap Java para o plug-in SnapCenter para VMware vSphere não for grande o suficiente, o backup pode 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 servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

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

   É apresentado o aviso de nome de utilizador e palavra-passe.

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 da tarefa (em execução, concluída ou com falha) usando o cmdlet Get-smJobSummaryReport.

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. Monitore os detalhes da tarefa de backup, como ID do backup, nome do backup para executar a operação de restauração ou clone 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*. Em alternativa, pode também consultar o "Guia de referência de 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 uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, 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 uma programação configurada, os backups ocorrerão automaticamente de acordo com a programação.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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 selecionando a tag. Em seguida, pode 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. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Monitore as operações de backup do PostgreSQL

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado correspondente das operações:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- 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 a que apenas as operações de cópia de segurança sejam listadas.

b. Especifique as datas de início e fim.

c. Na lista suspensa **Type**, selecione **Backup**.

d. Na lista suspensa **Status**, selecione o status da cópia de segurança.

e. Clique em **Apply** para ver as operações concluídas com êxito.

4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.

Embora o status do trabalho de backup seja exibido , quando você clica nos detalhes do trabalho, você pode ver que algumas das tarefas secundárias da operação de backup ainda estão em andamento ou marcadas com sinais de aviso.

5. Na página Detalhes da tarefa, clique em **Exibir logs**.

O botão **View logs** exibe os logs detalhados para a operação selecionada.

Monitore operações de proteção de dados em clusters PostgreSQL no painel atividade

O painel atividade exibe as cinco operações mais recentes executadas. O painel atividade também é exibido quando a operação foi iniciada e o status da operação.

O painel atividade exibe informações sobre operações de backup, restauração, clone e backup agendadas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 da tarefa**.

Cancelar operações de backup para PostgreSQL

Você pode cancelar as operações de backup que estão na fila.

O que você vai precisar

- Você deve estar logado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de cópia de segurança em execução.
- Você pode usar os comandos GUI, cmdlets do SnapCenter ou CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** está desativado 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 em fila de outros membros enquanto usa essa função.

Passos

1. Execute uma das seguintes ações:

A partir 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 da atividade	a. Depois de iniciar a operação de backup, clique em no painel atividade para exibir as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

A operação é cancelada e o recurso é revertido para o estado anterior.

Veja backups e clones do PostgreSQL na página topologia

Ao se preparar para fazer backup ou clonar um recurso, talvez seja útil exibir uma representação gráfica de todos os backups e clones no storage primário e secundário.

Sobre esta tarefa

Você pode revisar os ícones a seguir na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no storage primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups e clones disponíveis no storage primário.
- Exibe o número de backups e clones espelhados no storage secundário usando a tecnologia SnapMirror.
- Exibe o número de backups e clones replicados no storage secundário usando a tecnologia SnapVault.

O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou backups 6 usando uma política para reter apenas 4 backups, o número de backups exibidos é 6.

Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

Na página topologia, você pode ver todos os backups e clones disponíveis para o grupo de recursos ou

recursos selecionado. Você pode visualizar os detalhes desses backups e clones e, em seguida, selecioná-los para executar operações de proteção de dados.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o recurso ou o 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 de 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 baseados em cópia Snapshot.

   Clicar no botão **Refresh** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clique no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Um horário semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo é espalhado por vários volumes, o tempo de expiração do SnapLock para o backup será o tempo de expiração do SnapLock mais longo definido para um snapshot em um volume. O tempo de expiração mais longo do SnapLock é recuperado do ONTAP.

   Após o backup sob demanda, clicando no botão **Refresh** atualiza os detalhes do backup ou clone.

5. No modo de 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 um 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 estão no armazenamento secundário.

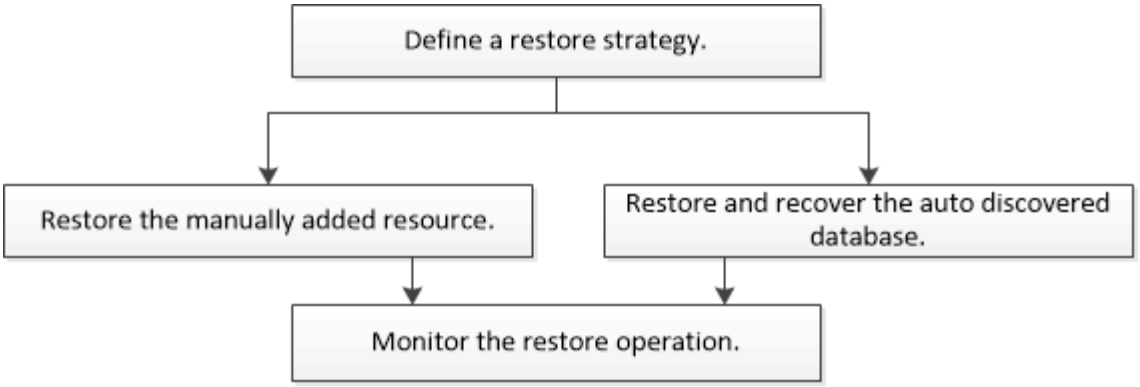
7. Se quiser excluir um clone, selecione-o na tabela e clique em .
8. Se quiser dividir um clone, selecione-o na tabela e clique em .

Restaure o PostgreSQL

Restaure o fluxo de trabalho

O fluxo de trabalho de restauração e recuperação inclui Planejamento, execução das 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 clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre cmdlets do PowerShell.

"Guia de referência de cmdlet do software SnapCenter".

Restaure e recupere um backup de recursos 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 dos grupos de recursos ou recursos.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos pré-restauração, pós restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização 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 a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com o tipo, host, grupos de recursos e políticas associados e status.

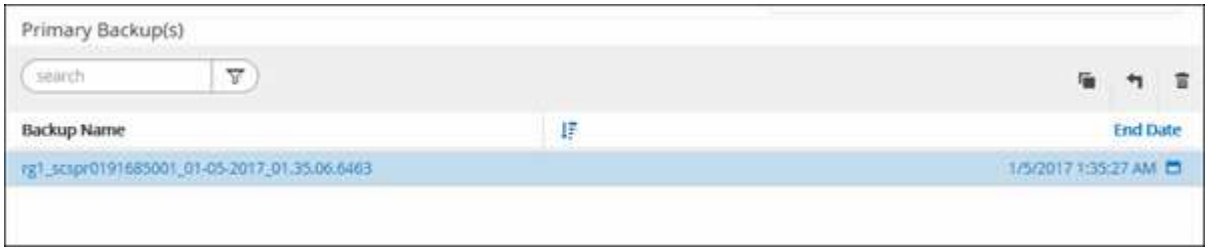
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, ""não protegido"" é exibido na coluna Estado geral. Isso pode significar que o recurso não está protegido ou que o recurso foi protegido 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 do recurso é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Na tabela de backup principal, selecione o backup do qual você deseja restaurar e clique em * * .



6. Na página Restaurar escopo, selecione **recurso completo**.

   a. Se você selecionar **Complete Resource**, todos os volumes de dados configurados do cluster PostgreSQL serão restaurados.

      Se o recurso contiver volumes ou qtrees, os instantâneos obtidos 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.

      Pode selecionar vários LUNs.

      Se você selecionar **All**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.

7. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar 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 a execução de 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 **Finish**.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 29th 2015 de janeiro a 3rd 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 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Restaure e recupere 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 dos grupos de recursos ou recursos.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos pré-restauração, pós restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter*

Plug-in Creator/etc/allowed_commands.config

- Localização 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

- As cópias de backup baseadas em arquivo não podem ser restauradas a partir do SnapCenter.
- Para recursos descoberta automática, a restauração é suportada com SFSR.
- A recuperação automática não é suportada.
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com o tipo, host, grupos de recursos e políticas associados e status.

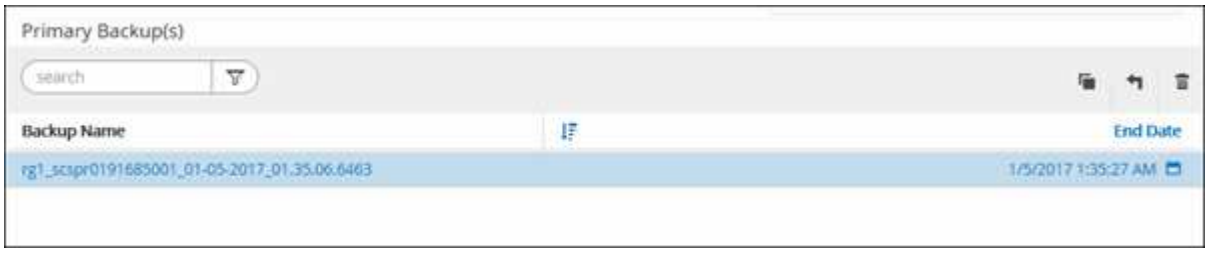
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, ""não protegido"" é exibido na coluna Estado geral. Isso pode significar que o recurso não está protegido ou que o recurso foi protegido 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 do recurso é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Na tabela de backup principal, selecione o backup do qual você deseja restaurar e clique em * * .



6. Na página Restaurar escopo, selecione **recurso completo** para restaurar os volumes de dados configurados do cluster PostgreSQL.
7. Na página âmbito de recuperação, selecione uma das seguintes opções:

Se você…	Faça isso…

Deseja recuperar o mais próximo possível da hora atual	Selecione **Recover to most recent State** (recuperar para o estado mais recente). Para recursos de contentor único, especifique um ou mais locais de backup de log e catálogo.
Deseja recuperar para o ponto especificado no tempo	Selecione **Recover to point in time**. a. Introduza a data e a hora. Introduza 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 deseja executar uma recuperação para 5 a.m .Sunnyvale, CA, então o usuário deve definir o fuso horário do navegador para o fuso horário do host PostgreSQL Linux, que é GMT-07:00 e especificar a data e hora como 5:00 a.m.
Não quero recuperar	Selecione **sem recuperação**.

Você não pode recuperar recursos PostgreSQL adicionados manualmente.

O plug-in SnapCenter para PostgreSQL cria uma pasta backup_label e tablespace_map na pasta */<OS_temp_folder>/postgresql_SC_recovery*<Restore_JobId>/_ para ajudar a recuperar manualmente.

1. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar 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 a execução de 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 **Finish**.
5. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Restaure recursos usando cmdlets do PowerShell

A restauração de um backup de recurso inclui iniciar uma sessão de conexão com o

servidor SnapCenter, listar os backups e recuperar informações de backup e 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 servidor SnapCenter 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 29th 2015 de janeiro a 3rd 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 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Monitore as operações de restauração do PostgreSQL

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um 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 executar.

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso

- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Restore**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Clonar backups de recursos do PostgreSQL

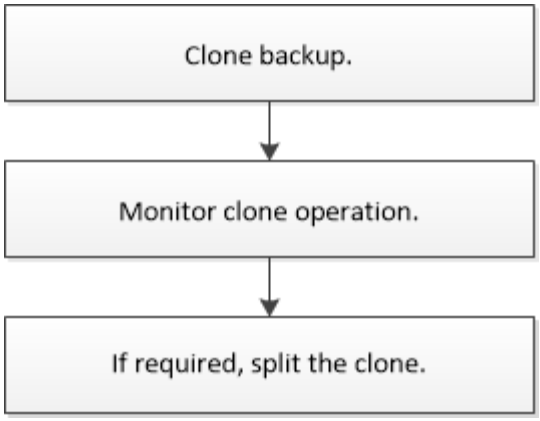
Fluxo de trabalho clone

O fluxo de trabalho do clone inclui a execução da operação de clone e o monitoramento da 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 de aplicativos
  - 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 clone:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre cmdlets do PowerShell.

Clonar um backup PostgreSQL

Você pode usar o SnapCenter para clonar um backup. Você pode clonar 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 storage (SVM).
- Para comandos pré-clone ou pós-clone, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização 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 limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com informações como tipo, host, grupos e políticas de recursos associados e status.

3. Selecione o grupo de recursos ou recursos.

   Você deve selecionar um recurso se selecionar um grupo de recursos.

   A página de topologia do grupo de recursos ou recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Selecione o backup de dados na 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-alvo	Insira a porta de destino PostgreSQL para clonar dos backups existentes.
Endereço IP de exportação NFS	Insira endereços IP ou os nomes de host nos quais os volumes clonados serão exportados. Isso é aplicável apenas ao recurso do tipo de storage NFS.
Taxa de transferência máx. Do pool de capacidade (MIB/s)	Insira a taxa de transferência máxima de um pool de capacidade. Isso se aplica apenas ao recurso do tipo de storage do ANF.

7. Na página Scripts, execute as seguintes etapas:

   Os scripts são executados no host do plug-in.

   a. Digite os comandos para pré-clone ou pós-clone que devem ser executados antes ou depois da operação clone, respetivamente.
      - Comando pré-clone: Exclua clusters existentes com o mesmo nome
      - Comando pós-clone: Verifique um cluster ou inicie um cluster.
   b. Digite o comando mount para montar um sistema de arquivos em um host.

Monte o comando 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 **Finish**.
10. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

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

2. Recupere os backups para executar a operação de clone 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 clone a partir de um backup existente e especifique os endereços IP de exportação NFS nos quais os volumes clonados são exportados.

   Este exemplo mostra que o backup a ser clonado tem um endereço NFSExportIPs de 10.32.212.14:

   Para o 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 clone.

4. Verifique se os backups foram clonados com sucesso usando o cmdlet Get-SmCloneReport para exibir os detalhes da tarefa clone.

   Você pode exibir 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          :
```

Monitore as operações de clone do PostgreSQL

Você pode monitorar o andamento das operações de clone do SnapCenter usando a página tarefas. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista para que apenas operações de clone sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Divida um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido torna-se independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clones em um clone intermediário.

  Por exemplo, depois de criar clone1 a partir de um backup de banco de dados, você pode criar um backup de clone1 e clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e não é possível executar a operação de divisão de clones no clone1. No entanto, você pode executar a operação de divisão de clones no clone2.

  Depois de dividir clone2, você pode executar a operação de divisão de clones no clone1 porque clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e as tarefas de clone do clone são excluídas.
- Para obter informações sobre limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .
- Certifique-se de que o volume ou o agregado no sistema de storage esteja on-line.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.

2. Na página **recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicativos 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 do recurso é exibida.

4. No modo de 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 deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

   A operação de divisão de clones deixa de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clones e tentar novamente a operação de divisão de clones.

   Se você quiser um tempo de enquete mais longo 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 que o SMCore busque o status da operação de divisão de clones. O valor é em milissegundos e o valor padrão é de 5 minutos.

   Por exemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

   A operação de inicialização dividida de clone falhará se o backup, a restauração ou outra divisão de clones estiver em andamento. Você deve reiniciar a operação de divisão de clones somente depois que as operações em execução estiverem concluídas.

Informações relacionadas

"O clone ou a verificação do SnapCenter falha com o agregado não existe"

Exclua ou divida clones do cluster do PostgreSQL após a atualização do SnapCenter

Após a atualização para o SnapCenter 4,3, você não verá mais os clones. Você pode excluir o clone ou dividir os clones da página topologia do recurso a partir do qual os clones foram criados.

Sobre esta tarefa

Se você quiser localizar o espaço físico 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-sprotectresource.
4. Selecione o recurso pai na página recursos.

   A página de topologia do recurso é exibida.

5. Na visualização Gerenciar cópias, selecione os clones nos sistemas de storage primário ou secundário (espelhado ou replicado).
6. Selecione os clones e clique para excluir clones ou clique para dividir os clones.
7. Clique em **OK**.

Proteja o 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 software NetApp SnapCenter que permite o gerenciamento de proteção de dados com reconhecimento de aplicativos 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 em seu ambiente SnapCenter.

O SnapCenter suporta configurações MySQL de instância única. 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 é instalado, você pode usar o SnapCenter com 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 disco a disco para conformidade com os padrões.

O plug-in do SnapCenter para MySQL é compatível com NFS e SAN em layouts de storage de arquivos do ONTAP e do Azure NetApp.

O VMDK ou o layout de armazenamento virtual são suportados.

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.
- Criar backups.
- Restauração a partir de backups.
- Backups de clones.
- Agendar operações de backup.
- Monitore operações de backup, restauração e clone.
- Exibir relatórios para operações de backup, restauração e clone.

Plug-in do SnapCenter para recursos MySQL

O SnapCenter se integra à aplicação plug-in e às tecnologias NetApp no sistema de storage. Para trabalhar com o Plug-in para Banco de dados MySQL, você usa a interface gráfica do usuário do SnapCenter.

- * Interface gráfica unificada do usuário*

  A interface do SnapCenter fornece padronização e consistência em plug-ins e ambientes. A interface do SnapCenter permite concluir operações consistentes de backup, restauração e clone em plug-ins, usar relatórios centralizados, usar visualizações de painel rápidas, configurar controle de acesso baseado em funções (RBAC) e monitorar tarefas em todos os plug-ins.

- * Administração central automatizada*

  Você pode agendar operações de backup, configurar a retenção de backup baseada em política e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- **Tecnologia de cópia Snapshot NetApp sem interrupções**

  O SnapCenter usa a tecnologia NetApp snapshot 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 a fluxos de trabalho de backup, restauração e clone
- Delegação de funções centralizada e segurança compatível com RBAC

  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 uso eficiente de espaço e pontuais para teste ou extração de dados usando a tecnologia NetApp FlexClone

  É necessária uma licença FlexClone no sistema de storage onde você deseja criar o clone.

- Suporte para o recurso instantâneo do grupo de consistência (CG) do ONTAP como parte da criação de backups.
- Funcionalidade de executar vários backups simultaneamente em vários hosts de recursos

  Em uma única operação, os snapshots são consolidados quando os recursos em um único host compartilham o mesmo volume.

- Capacidade de criar instantâneos usando comandos externos.
- Suporte para Linux LVM no sistema de arquivos XFS.

Tipos de armazenamento suportados pelo plug-in SnapCenter para MySQL

O SnapCenter oferece suporte a uma ampla variedade de tipos de armazenamento em máquinas físicas e máquinas virtuais (VMs). Você deve verificar o suporte para o seu tipo de armazenamento antes de instalar o plug-in SnapCenter para MySQL.

Máquina	Tipo de armazenamento
Servidor físico	• LUNs conectados a FC • LUNs ligados ao iSCSI • Volumes conectados a NFS
VMware ESXi	• LUNs RDM conetados por um FC ou iSCSI ESXi HAScanning de adaptadores de barramento de host (HBAs) pode levar muito tempo para ser concluído 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** para 1 para reexaminar somente os HBA listados em HBA_DRIVER_NAMES. • ISCSI LUNs ligados diretamente ao sistema convidado pelo iniciador iSCSI • VMDKs em armazenamentos de dados NFS • VMDKs no VMFS criado • Volumes NFS conectados diretamente ao sistema convidado • Armazenamentos de dados da VVol em NFS e SAN O armazenamento de dados da VVol só pode ser provisionado com as Ferramentas do ONTAP para o VMware vSphere.

ONTAP Privileges mínimo necessário para o plug-in MySQL

Os ONTAP Privileges mínimos necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
  - event generate-AutoSupport-log
  - mostra o histórico de trabalhos
  - paragem do trabalho
  - lun
  - lun criar
  - lun criar

- lun criar
- eliminação lun
- lun igrop add
- lun igrop criar
- eliminação do agrupamento lun
- mudar o nome do grupo lun
- mudar o nome do grupo lun
- show de grupos de lun
- nós complementares de mapeamento de lun
- mapeamento lun criar
- eliminação do mapeamento lun
- mapeamento lun remove-reporting-nonos
- mostra de mapeamento lun
- modificação de lun
- movimentação de lun no volume
- lun offline
- lun online
- limpeza da reserva persistente de lun
- redimensionar lun
- série lun
- mostra lun
- regra adicional de política do SnapMirror
- regra de modificação de política do SnapMirror
- regra de remoção da política do SnapMirror
- SnapMirror policy show
- restauração de SnapMirror
- SnapMirror show
- SnapMirror show-history
- atualização do SnapMirror
- SnapMirror update-ls-set
- SnapMirror lista-destinos
- versão
- clone de volume criar
- show de clone de volume
- início da divisão do clone de volume
- paragem dividida clone volume
- criar volume

    - destruição de volume
    - clone de arquivo de volume criar
    - show-disk-use do arquivo de volume
    - volume off-line
    - volume online
    - modificação do volume
    - criar qtree de volume
    - eliminação de qtree de volume
    - modificação de qtree de volume
    - apresentação de qtree de volume
    - restrição de volume
    - apresentação do volume
    - criar instantâneo de volume
    - eliminar instantâneo do volume
    - modificação do instantâneo do volume
    - tempo de expiração do volume snapshot modify-SnapLock
    - mudar o nome do instantâneo do volume
    - restauração de snapshot de volume
    - restauração de arquivo de snapshot de volume
    - apresentação de instantâneo do volume
    - desmontar o volume
    - svm cifs
    - compartilhamento cifs de svm criar
    - exclusão de compartilhamento cifs de svm
    - apresentação do shadowcopy cifs de svm
    - exibição de compartilhamento cifs de svm
    - mostra cifs de svm
    - política de exportação de svm
    - criação de política de exportação de svm
    - exclusão da política de exportação do svm
    - regra de política de exportação de svm criar
    - a regra de política de exportação do svm é exibida
    - exibição da política de exportação do svm
    - svm iscsi
    - apresentação da ligação iscsi de svm
    - mostra o svm
- Comandos somente leitura: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior

- interface de rede
- mostra da interface de rede
- svm

Preparar sistemas de storage para replicação SnapMirror e SnapVault para MySQL

Você pode usar um plug-in do 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 disco a disco para conformidade com os padrões e outros fins relacionados à governança. Antes de executar essas tarefas, você deve configurar uma relação de proteção de dados entre os volumes de origem e destino e inicializar a relação.

O SnapCenter executa as atualizações para o SnapMirror e o SnapVault após concluir a operação de captura instantânea. As atualizações SnapMirror e SnapVault são executadas como parte da tarefa SnapCenter; não crie uma agenda ONTAP separada.

Se você estiver vindo para o SnapCenter de um produto NetApp SnapManager e estiver satisfeito com as relações de proteção de dados que configurou, ignore esta seção.

Uma relação de proteção de dados replica dados no storage primário (o volume de origem) para o storage secundário (o volume de destino). Ao inicializar a relação, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não suporta relações em cascata entre volumes SnapMirror e SnapVault (**Primary** > **Mirror** > **Vault**). Você deve usar relacionamentos de fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis de versão e como configurá-los, consulte "Documentação do ONTAP".

Estratégia de backup para MySQL

Defina uma estratégia de backup para MySQL

Definir uma estratégia de backup antes de criar seus trabalhos de backup ajuda a ter os backups necessários para restaurar ou clonar seus recursos com êxito. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (rto) e objetivo do ponto de restauração (RPO) determinam em grande parte a sua estratégia de backup.

Sobre esta tarefa

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. Rto é o momento em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a era dos arquivos que precisam 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 de seus recursos.

2. Decida quantos trabalhos de cópia de segurança necessita.
3. Decida como nomear seus backups.
4. Decida se você deseja criar uma política baseada em cópia Snapshot para fazer backup de snapshots consistentes com aplicativos do banco de dados.
5. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção a longo prazo.
6. Determine o período de retenção dos snapshots no sistema de storage de origem e no destino do SnapMirror.
7. Determine se deseja executar quaisquer comandos antes ou depois da operação de backup e forneça um prescritor ou postscript.

Descoberta automática de recursos no host Linux

Recursos são instâncias MySQL no host Linux que são gerenciadas pelo SnapCenter. Depois de instalar o plug-in do SnapCenter para MySQL, as instâncias do MySQL nesse host são descobertas e exibidas automaticamente na página recursos.

Tipos de backups suportados

Tipo de backup especifica o tipo de backup que você deseja criar. O SnapCenter suporta o tipo de backup baseado em cópia de snapshot para bancos de dados MySQL.

Backup baseado em cópia snapshot

Os backups baseados em cópias snapshot utilizam a tecnologia Snapshot da NetApp para criar cópias on-line e somente leitura dos volumes nos quais os bancos de dados MySQL residem.

Como o plug-in do SnapCenter para MySQL usa snapshots de grupos de consistência

Você pode usar o plug-in para criar snapshots de grupo de consistência para grupos de recursos. Um grupo de consistência é um contentor que pode abrigar vários volumes para que você possa gerenciá-los como uma entidade. Um grupo de consistência são snapshots 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 **descontraído**. Você também pode ativar ou desativar a sincronização WAFL (Write Anywhere File Layout) durante uma operação consistente de snapshot em grupo. O WAFL Sync melhora o desempenho de um snapshot de grupo de consistência.

Como o SnapCenter gerencia o gerenciamento de backups de log

O SnapCenter gerencia o gerenciamento de backups de dados nos níveis do sistema de storage e do sistema de arquivos.

Considerações para determinar agendas de backup para MySQL

O fator mais crítico na determinação de um agendamento de backup é a taxa de

alteração do recurso. Você pode fazer backup de um recurso muito usado a cada hora, enquanto você pode fazer backup de um recurso raramente usado uma vez por dia. Outros fatores incluem a importância do recurso para a sua organização, seu contrato de nível de serviço (SLA) e seu objetivo do ponto de restauração (RPO).

Os programas de backup têm duas partes, como segue:

- Frequência de backup (com que frequência os backups devem ser executados)

  A frequência de backup, também chamada de tipo de programação para alguns plug-ins, faz parte de uma configuração de política. Por exemplo, você pode configurar a frequência de backup como hora, dia, semanal ou mensal.

- Programações de backup (exatamente quando os backups devem ser executados)

  As agendas de backup fazem parte de uma configuração de recurso ou grupo de recursos. Por exemplo, se você tiver um grupo de recursos que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas

Número de tarefas de backup necessárias para o MySQL

Os fatores que determinam o número de tarefas de backup de que você precisa 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 MySQL

Você pode usar a convenção padrão de nomenclatura Snapshot ou usar uma convenção de nomenclatura personalizada. A convenção de nomenclatura de backup padrão adiciona um carimbo de data/hora aos nomes de Snapshot 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 carimbo de data/hora.

Como alternativa, você pode especificar o formato do nome da captura Instantânea enquanto protege recursos ou grupos de recursos selecionando **usar formato de nome personalizado para cópia Instantânea**. Por exemplo, customtext_resourcegroup_policy_hostname ou resourcegroup_hostname. Por

padrão, o sufixo do carimbo de hora é adicionado ao nome do instantâneo.

Estratégia de restauração e recuperação para MySQL

Defina 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 você possa executar operações de restauração e recuperação com sucesso.

Somente a recuperação manual do banco de dados é suportada.

Passos

1. Determine as estratégias de restauração suportadas para recursos MySQL adicionados manualmente
2. Determine 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 executar operações de restauração com êxito usando o SnapCenter. Existem dois tipos de estratégias de restauração para recursos MySQL adicionados manualmente.

Você não pode 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 obtidos após o snapshot selecionado para restauração em tais 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 executar operações de restauração com êxito usando o SnapCenter.

A restauração completa de recursos é a estratégia de restauração suportada para 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 do SnapCenter para MySQL suporta SnapRestore de arquivo único e tipos de restauração de conexão e cópia para bancos de dados MySQL descobertos automaticamente.

O SnapRestore de arquivo único é executado em ambientes NFS para os seguintes cenários:

- Se apenas a opção **Complete Resource** estiver selecionada
- Quando o backup selecionado é de um local secundário SnapMirror ou SnapVault e a opção **recurso completo** está selecionada

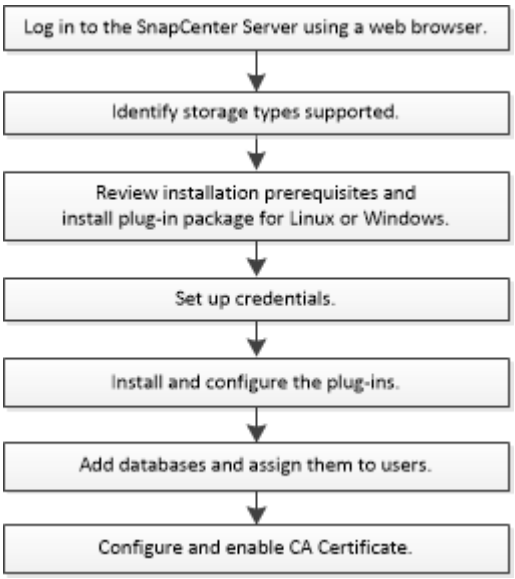
O SnapRestore de Arquivo único é executado em ambientes SAN para os seguintes cenários:

- Se apenas a opção **Complete Resource** estiver selecionada
- Quando o backup é selecionado em um local secundário do SnapMirror ou do SnapVault e a opção **recurso completo** está 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 plug-in SnapCenter para MySQL se quiser proteger bancos de dados MySQL.



Pré-requisitos para adicionar hosts e instalar o plug-in SnapCenter para MySQL

Antes de adicionar um host e instalar os pacotes de plug-in, você deve completar todos os requisitos. O plug-in SnapCenter para MySQL está disponível em ambientes Windows e Linux.

- Você deve ter instalado o Java 11 em seu host.

  O IBM Java não é suportado.

- Para 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 do Windows, se você especificar uma credencial que não está

integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host. O plug-in SnapCenter para Microsoft Windows será implantado por padrão com o plug-in MySQL em hosts Windows.

- O servidor SnapCenter deve ter acesso ao 8145 ou à porta personalizada do plug-in para host MySQL.
- Para o MySQL 5,7, binlog deve ser especificado no arquivo mysql config (my.cnf ou mysql-server.cnf).

Hosts do Windows

- Você deve ter um usuário de domínio com Privileges de administrador local com permissões de login local no host remoto.
- Ao instalar o plug-in para MySQL em um host Windows, o plug-in SnapCenter 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 em seu host Windows.

  "Downloads Java para todos os sistemas operacionais"

  "Ferramenta de Matriz de interoperabilidade do 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 em seu host Linux.

  "Downloads Java para todos os sistemas operacionais"

  "Ferramenta de Matriz de interoperabilidade do NetApp"

- Para bancos de dados MySQL que estão sendo executados em um host Linux, ao instalar o plug-in para MySQL, o plug-in SnapCenter para UNIX é instalado automaticamente.
- Você deve ter **bash** como o shell padrão para instalação do plug-in.

Comandos suplementares

Para executar um comando complementar no plug-in do SnapCenter para MySQL, você deve incluí-lo no arquivo *allowed_commands.config*.

- Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
- Localização 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 são sensíveis a maiúsculas e minúsculas. Certifique-se de especificar o nome de caminho totalmente qualificado e incluir o nome de caminho entre aspas (") se ele contiver espaços.

Por exemplo:

Comando: Comando de montagem: Comando umount: Comando "C: Arquivos de programas/NetApp comandos do SnapCreator" comando: myscript.bat

Se o arquivo *allowed_commands.config* não estiver presente, os comandos ou a execução de 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.

Configure sudo Privileges 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 de plug-in serão executados como um usuário não-root eficaz. Você deve configurar o sudo Privileges para que o usuário não-root forneça acesso a vários caminhos.

O que você vai precisar

- Sudo versão 1.8.7 ou posterior.
- Se o umask for 0027, certifique-se de que a pasta java e todos os arquivos dentro devem ter permissão de 555. Caso contrário, a instalação do plug-in pode falhar.
- Para o usuário não-root, certifique-se de que o nome do usuário não-root e do grupo do usuário devem ser os mesmos.
- Edite o arquivo */etc/ssh/sshd_config* para configurar os algoritmos de código de autenticação de mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

  Reinicie o serviço sshd depois de 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 o sudo Privileges para que o usuário não-root forneça acesso aos seguintes caminhos:

- /Home/*Linux_USER*/.SC_NetApp/SnapCenter_linux_host_plugin.bin
- /Custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/SnapCenter/spl/bin/spl

Passos

1. Faça 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 !visiblepw
Defaults: LINUX_USER !requiretty
```

Se você estiver tendo uma configuração RAC, juntamente 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**, que está localizado em:

- _C: /ProgramData/NetApp/SnapCenter/Repositório de pacotes/sc_unix_plugins_checksum.txt _ se o servidor SnapCenter estiver instalado no host do Windows.
- _/opt/NetApp/SnapCenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ se o servidor SnapCenter 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 do 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 do sistema host e requisitos de dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.
Pacotes de software necessários	• DOTNET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell Core 7.4.2 Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet."

Requisitos de host para instalar o pacote de plug-ins do SnapCenter para Linux

Antes de instalar o pacote de plug-ins do 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 • SUSE Linux Enterprise Server (SLES) Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto. Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Configure 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 raiz ou para um usuário não-root que tenha sudo Privileges para instalar e iniciar o processo de plug-in.

Prática recomendada: embora você tenha permissão para criar credenciais para Linux após implantar hosts e instalar plug-ins, a prática recomendada é criar credenciais após adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

  Você deve configurar as credenciais do Windows antes de instalar os plug-ins.

  Você deve configurar as credenciais com o Privileges 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 Privileges de administrador completo, será necessário atribuir pelo menos o grupo de recursos e Privileges de backup ao nome de usuário.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Clique em **novo**.
4. Na página Credential (credencial), especifique as informações necessárias para configurar credenciais:

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para as credenciais.

Para este campo…	Faça isso…
Nome de utilizador	Introduza o nome de utilizador e a palavra-passe a utilizar para a 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 no qual você está instalando o plug-in do SnapCenter. Formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS_username* ◦ *Domain FQDN_username* • Administrador local (apenas para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é: *Nome de usuário* Não use aspas duplas (") ou backtick (') nas senhas. Você não deve usar os símbolos menos de (>) e exclamação (!) juntos em senhas. Por exemplo, lessthan!10, lessthan10You!, backtick'12.
Palavra-passe	Introduza a palavra-passe utilizada para autenticação.
Modo de autenticação	Selecione o modo de autenticação que pretende utilizar.
Use sudo Privileges	Marque a caixa de seleção **Use sudo Privileges** se estiver criando credenciais para um usuário que não seja root. Aplicável apenas a usuários 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.

Instale o plug-in SnapCenter para MySQL

Adicione hosts e instale pacotes plug-in 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 servidor SnapCenter for o Windows 2019 e o sistema operacional do host do plug-in for o Windows 2022, você deve executar o seguinte:
  - Atualize para o Windows Server 2019 (versão de SO 17763,5936) ou posterior
  - Atualize para o Windows Server 2022 (versão de SO 20348,2402) ou posterior
- Você deve ser um usuário atribuído a uma função que tenha as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar 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 servidor SnapCenter como um host plug-in a outro servidor SnapCenter.

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Verifique se a guia **hosts gerenciados** está selecionada na parte superior.
3. Clique em **Add**.
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 tem que ser instalado no servidor de banco de dados MySQL.

Para este campo…	Faça isso…
Nome do host	Insira o nome do host de comunicação. Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no 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 exibir detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você forneceu. 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 instalar.

   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	Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido 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, você deve especificar a mesma porta. Caso contrário, a operação falha.

Para este campo…	Faça isso…
Caminho de instalação	O Plug-in para MySQL é instalado no host cliente MySQL, e este host pode estar em um sistema Windows ou em um sistema Linux. • Para o pacote de plug-ins do 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 do SnapCenter para Linux, o caminho padrão é /opt/NetApp/SnapCenter. Opcionalmente, você pode personalizar o caminho.
Ignorar as verificações de pré-instalação	Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.
Adicione todos os hosts no cluster	Não aplicável.
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	Não aplicável.

7. Clique em **Enviar**.

   Se você não tiver selecionado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se o host 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 Java (para plug-ins do Linux) são validados de acordo com os requisitos mínimos. Se os requisitos mínimos não forem cumpridos, são apresentadas mensagens de erro ou de aviso adequadas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado no NetApp SnapCenter para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, será necessário atualizar o arquivo em ambos os nós.

8. Se o tipo de host for Linux, verifique a impressão digital e clique em **Confirm and Submit**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós no cluster.

   A verificação de impressões digitais é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitorize o progresso da instalação.
   - Para o plug-in do Windows, os logs de instalação e atualização estão localizados em: *C: Plug-in do Windows SnapCenter*<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 de terminar

Se você quiser atualizar para a versão do SnapCenter 6,0, o plug-in baseado EM PERL existente para MySQL será desinstalado do servidor de plug-in remoto.

Instale pacotes de plug-ins do 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 PowerShell.

Antes de começar

Você deve ter feito 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 servidor SnapCenter, 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*. Em alternativa, pode também consultar o "Guia de referência de 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 do SnapCenter para banco de dados MySQL usando a interface de usuário do SnapCenter (UI). Se o seu ambiente não permitir a instalação remota do plug-in a partir da IU do SnapCenter, você pode instalar o plug-in para banco de dados MySQL no modo console ou no modo silencioso usando a interface de linha de comando (CLI).

Antes de começar

- Você deve instalar o Plug-in para MySQL Database em cada um dos hosts Linux onde a instância MySQL deve ser protegida.
- O host Linux no qual você está instalando o plug-in SnapCenter 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 do NetApp"

- O plug-in do SnapCenter para banco de dados MySQL faz parte do pacote de plug-ins do SnapCenter para Linux. Antes de instalar o pacote de plug-ins do SnapCenter para Linux, você já deve ter instalado o SnapCenter em um host do Windows.

Passos

1. Copie o pacote de plug-ins do SnapCenter para o arquivo de instalação do Linux (SnapCenter_linux_host_plugin.bin) de C:/NetApp/SnapCenter para o host onde você deseja instalar o plug-in para o MySQL.

   Você pode acessar esse caminho a partir do host onde o servidor SnapCenter 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 SMCore.
   - -DSERVER_IP especifica o endereço IP do servidor SnapCenter.
   - -DSERVER_HTTPS_PORT especifica a porta HTTPS do servidor SnapCenter.
   - -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 /<installation directory>/NetApp/SnapCenter/scc/etc/SC_SMS_Services.properties e, em seguida, adicione o parâmetro PLUGINS_ENABLED: MySQL:3,0.
5. Adicione o host ao servidor SnapCenter 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Monitore o status da instalação do Plug-in para MySQL

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
   a. Clique em **filtro**.
   b. Opcional: Especifique a data de início e fim.
   c. No menu suspenso tipo, selecione **Instalação 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 **Visualizar logs**.

Configurar certificado CA

Gerar arquivo CSR do 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 a CSR gerada. O certificado terá uma chave privada associada a ele.

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

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

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

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

Para configurações de cluster, o nome do cluster (FQDN de cluster virtual) e os respetivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome alternativo (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados CA

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 **Yes**, importe a chave privada e clique em **Next**.
Importar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

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

7. Repita o passo 5 para a pasta "Pessoal".

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia 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 **thumbprint**.
   d. Copie os carateres 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

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.

Configure o certificado CA com os serviços de plug-in do host do Windows

Você deve configurar o certificado CA com os serviços de plug-in host do Windows para ativar o certificado digital instalado.

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, 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"
   ```

Configure o certificado CA para o serviço de plug-ins MySQL do SnapCenter 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. Altere a senha do keystore:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Altere a senha para 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 depois de 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. Liste 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 de CA raiz e, em seguida, os certificados de CA intermediários.

Configurar o par de chaves assinadas pela CA para plug-in de armazenamento confiável

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. Liste 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. Liste os certificados adicionados no keystore.

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

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

   A senha padrão do keystore 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 espaço ou
carateres 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 com a chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o plug-in trust-store.

Configurar a lista de revogação de certificados (CRL) para plug-ins do SnapCenter

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 SnapCenter é 'opt/NetApp/snapcenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties contra a chave CRL_PATH.

   Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Configure o certificado CA para o serviço de plug-ins MySQL do SnapCenter 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 Plug-ins 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. Altere 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 por seu caminho completo.

   C: Arquivos de programas/<jdk_version>/keytool.exe" -storepasswd -keystore keystore.jks

3. Altere a senha para 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*.

4. Reinicie o serviço depois de 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. Liste 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 de CA raiz e, em seguida, os certificados de CA intermediários.

Configurar o par de chaves assinadas pela CA para plug-in de armazenamento confiável

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. Liste 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 -destinkeystore keystore.jks -deststoretype JKS

5. Liste os certificados adicionados no keystore.

   keytool -list -v -keystore keystore.jks

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da 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

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

   Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o plug-in trust-store.

Configurar a lista de revogação de certificados (CRL) para plug-ins do SnapCenter

Sobre esta tarefa

- Para transferir o ficheiro CRL mais recente para o certificado CA relacionado, "Como atualizar o arquivo de lista de revogação de certificados no certificado da CA do SnapCenter"consulte .
- 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* contra a chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

   Os certificados recebidos serão verificados em relação a cada CRL.

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet RUN *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando as *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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- * * Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.

- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da 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 são concluídas com êxito.

Preparar-se para a proteção de dados

Pré-requisitos para usar o plug-in SnapCenter para MySQL

Antes de usar o plug-in do SnapCenter para MySQL, o administrador do SnapCenter deve instalar e configurar o servidor SnapCenter e executar as tarefas de pré-requisito.

- Instalar e configurar o servidor SnapCenter.
- Inicie sessão no servidor SnapCenter.
- Configure o ambiente SnapCenter adicionando conexões do sistema de storage e criando credenciais, se aplicável.
- Instale o Java 11 em seu host Linux ou Windows.

  Você deve definir o caminho Java na variável caminho ambiental da máquina host.

- Configure o SnapMirror e o SnapVault, se quiser replicação de backup.

Como recursos, grupos de recursos e políticas são usados para proteger o MySQL

Antes de usar o SnapCenter, é útil entender 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 clonar com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host.

  Quando você executa uma operação em um grupo de recursos, executa essa operação nos recursos definidos no grupo de recursos de acordo com a programação especificada 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 programados para recursos únicos e grupos de recursos.

- As políticas especificam a frequência do backup, a replicação, os scripts e outras caraterísticas 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 quando você executa um backup sob demanda para um único recurso.

Pense em um grupo de recursos como definindo o que você quer proteger e quando você quer protegê-lo em termos de dia e tempo. Pense em uma política como definir 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

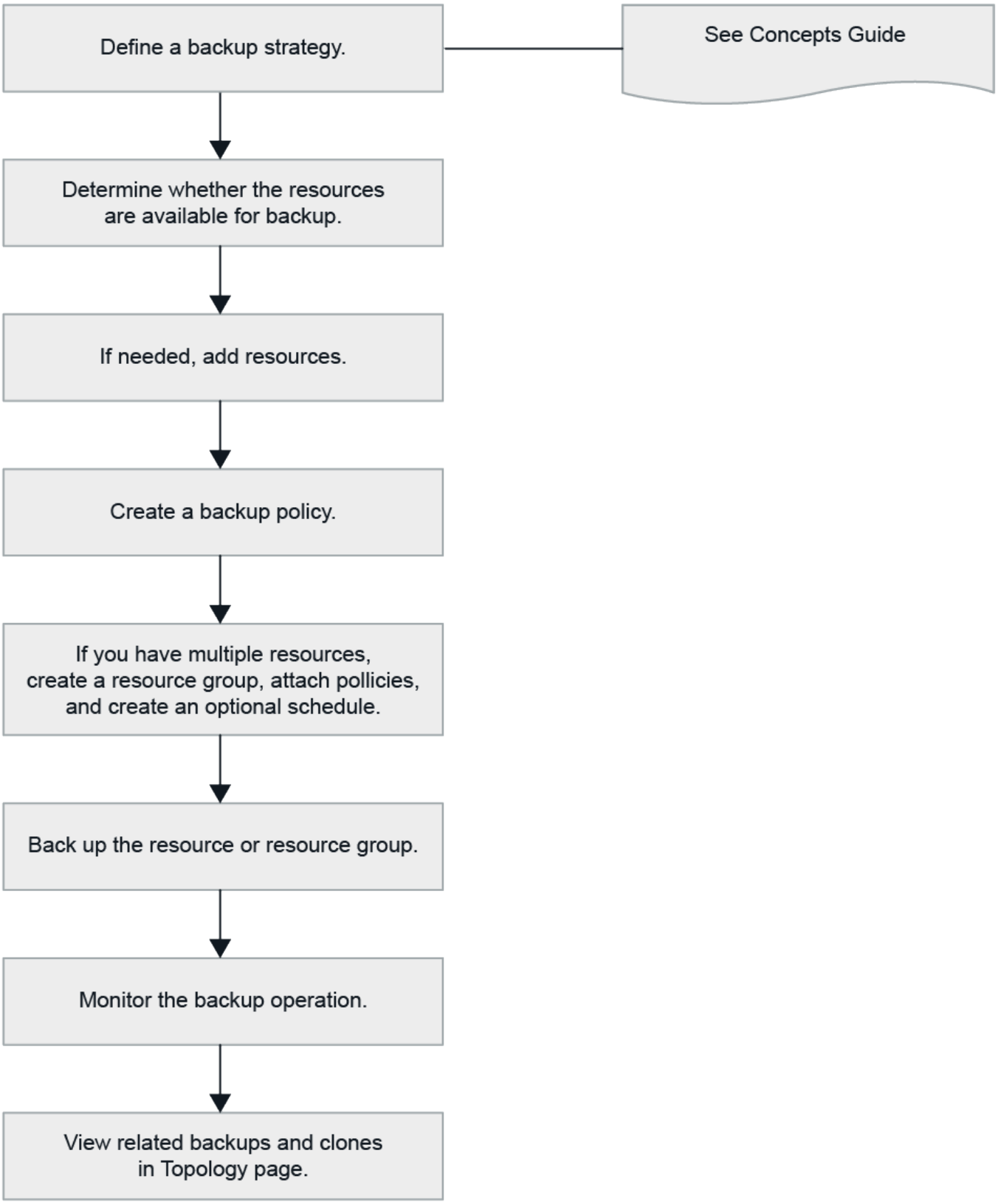
todos os bancos de dados no host. Em seguida, você pode anexar duas políticas ao grupo de recursos: Uma política diária e uma política por hora. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup completo diariamente.

Faça backup de recursos MySQL

Faça backup de recursos 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 de bancos de dados para backup, gerenciamento de políticas de backup, criação de grupos de recursos e inclusão 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 clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell. "Guia de referência de cmdlet do software SnapCenter".

Descubra os bancos de dados automaticamente

Recursos são bancos de dados MySQL no host Linux que são gerenciados pelo SnapCenter. Você pode adicionar os recursos a 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 servidor SnapCenter, adicionar hosts e configurar as conexões do sistema de armazenamento.
- O plug-in SnapCenter para MySQL não suporta a descoberta automática dos recursos residentes em ambientes virtuais RDM/VMDK. Você deve fornecer as informações de storage para ambientes virtuais e adicionar os bancos de dados manualmente.

Sobre esta tarefa

- Depois de instalar o plug-in, todos os bancos de dados nesse host Linux são automaticamente descobertos e exibidos na página recursos.
- Somente bancos de dados são auto-descobertos.

Os recursos descobertos automaticamente não podem ser modificados ou excluídos.

Passos

1. No painel de navegação à esquerda, clique em **Resources** 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 selecione o nome do host.

   Em seguida, pode clicar em* * para fechar o painel do filtro.

4. Clique em **Atualizar recursos** para descobrir os recursos disponíveis no host.

   Os recursos são exibidos juntamente 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, então não protegido será exibido na coluna Estado geral.
   - Se o banco de dados estiver em um sistema de armazenamento NetApp e protegido, e se não houver operação de backup executada, o Backup não executado será exibido na coluna Estado geral. O status mudará para Backup failed ou Backup successful com base no último status de backup.

Você deve atualizar os recursos se as instâncias forem renomeadas fora do SnapCenter.

Adicione recursos manualmente ao host do plug-in

A deteção automática não é suportada no host Windows. Você deve adicionar instâncias MySQL e recursos de banco de dados manualmente.

Antes de começar

- Você deve ter concluído tarefas como instalar o servidor SnapCenter, adicionar hosts e configurar conexões do sistema de armazenamento.

Passos

1. No painel de navegação à esquerda, selecione o plug-in SnapCenter para MySQL na lista suspensa e clique em **recursos**.
2. Na página recursos, clique em **Adicionar recursos 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	Insira o nome do host.
Tipo	Selecione instância.
Instância	Não aplicável.
Credenciais	Selecione as credenciais ou adicione informações para a credencial. Isso é opcional.

4. Na página fornecer espaço físico 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 **Finish**.

   Os bancos de dados são exibidos juntamente com informações como o nome do host, grupos e políticas de recursos associados e status geral

Se você quiser fornecer aos usuários acesso a recursos, você deve atribuir os recursos aos usuários. Isso permite que os usuários executem as ações para as quais eles têm permissões nos ativos que são atribuídos a eles.

"Adicione um usuário ou grupo e atribua funções 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 MySQL, você deve criar uma política de backup para o grupo de recursos ou recursos que deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e retém backups.

Antes de começar

- Você precisa 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 precisa se preparar para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, configurar conexões do sistema de storage e adicionar recursos.
- O administrador do SnapCenter deve ter atribuído os SVMs para os volumes de origem e destino a você se estiver replicando snapshots em um espelho ou cofre.

  Além disso, você pode especificar as 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 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio de instantâneos impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na política.
  - Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

As configurações do SnapLock primário são gerenciadas na política de backup do SnapCenter e as configurações do SnapLock secundário são gerenciadas pelo ONTAP.

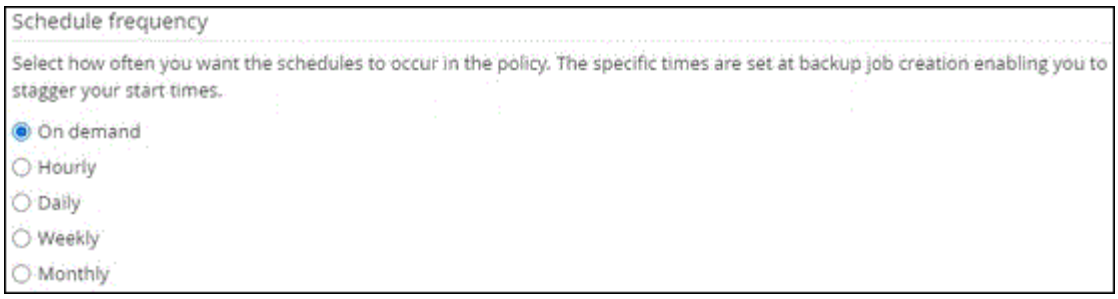
Passos

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 a descrição da política.
5. Na página tipo de política, execute o seguinte:
   a. Selecione o tipo de armazenamento.
   b. Na seção **Configurações personalizadas de backup**, forneça quaisquer configurações específicas de backup que tenham que ser passadas para o formato de valor de chave do plug-in.

      Você pode fornecer vários valores-chave a serem passados para o plug-in.

6. Na página Snapshot, especifique o tipo de agendamento selecionando **On Demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.

Você pode especificar a programação (data de início, data de término e frequência) para a operação de backup enquanto cria 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 programações de backup a cada política.



Se você tiver agendado para as 2:00 da manhã, o horário não será acionado durante o horário de verão (DST).

7. Na seção Configurações de instantâneos, especifique o número de instantâneos que você deseja manter.
8. Na página retenção, 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 instantâneos	Selecione **Copies to keep** e especifique o número de instantâneos que deseja manter. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro.

Para backups baseados em cópias Snapshot, defina a contagem de retenção para 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção pode falhar porque o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino.

9. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas

Um grupo de recursos é o contentor ao qual você deve adicionar recursos que deseja fazer backup e proteger. Um grupo de recursos permite fazer 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 tarefa de proteção de dados que deseja executar.

Sobre esta tarefa

- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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	Introduza um nome para o grupo de recursos. O nome do grupo de recursos não deve exceder 250 carateres.
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.
Use o formato de nome personalizado para cópia instantânea	Marque essa 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 carimbo de data/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 **Resource Type**.

   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:

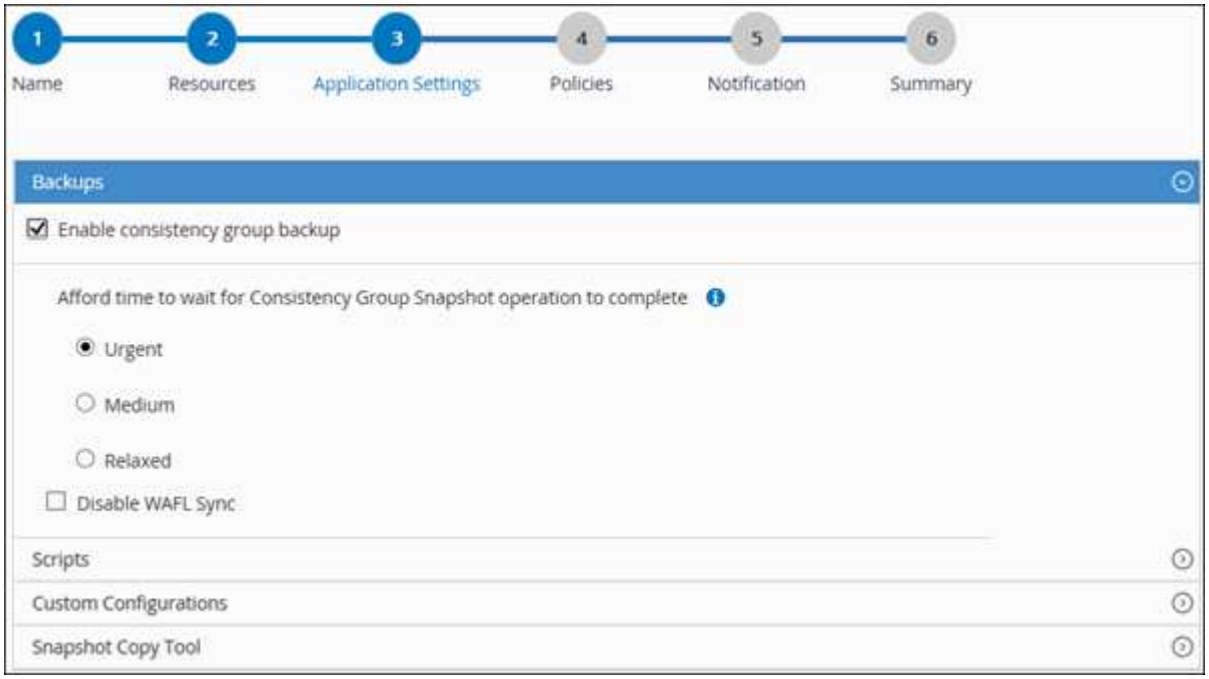
   a. Clique na seta **backups** para definir opções adicionais de backup:

      Ative o backup do grupo de consistência e execute as seguintes tarefas:

Para este campo…	Faça isso…
Tenha tempo para esperar que a operação de snapshot do Grupo de consistência seja concluída	Selecione **urgente**, **Médio** ou **relaxado** para especificar o tempo de espera para que a operação de snapshot seja concluída. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.

Para este campo…	Faça isso…
Desativar a 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 quiesce, snapshot e unquiesce. Também pode introduzir os pré comandos a serem executados antes de sair em caso de falha.

b. Clique na seta **Custom Configurations** (Configurações personalizadas) e insira os pares de valor de chave personalizados necessários para todas as operações de proteção de dados usando esse recurso.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_ENABLE	(Y/N)	Permite que a gestão do registo de arquivo elimine os registos de arquivo.
ARCHIVE_LOG_RETENÇÃO	number_of_days	Especifica o número de dias em que os logs de arquivo são mantidos. Esta definição tem de ser igual ou superior a NTAP_SNAPSHOT_ RETENÇÕES.
ARCHIVE_LOG_DIR	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs do arquivo.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_EXT	extensão_ficheiro	Especifica o comprimento da extensão do arquivo de log do arquivo. Por exemplo, se o log de arquivo for log_backup_0_0_0_0,161518551942 9 e se o valor file_extension for 5, a extensão do log manterá 5 dígitos, que é 16151.
ARCH ARCHIVE_LOG_RECURSIVE_SE	(Y/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs do arquivo estiverem localizados em subdiretórios.

Os pares de chave-valor personalizados são suportados para sistemas de plug-in MySQL Linux e não são suportados para banco de dados MySQL registrado como um plug-in centralizado do Windows.

c. Clique na seta **Snapshot Copy Tool** 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, essa opção não é aplicável.	Selecione **SnapCenter com consistência do sistema de arquivos**.
SnapCenter para criar um instantâneo de nível de storage	Selecione **SnapCenter sem consistência do sistema de arquivos**.
Para inserir o comando a ser executado no host para criar cópias snapshot.	Selecione **Other** e, em seguida, digite 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 programações para políticas selecionadas.

b.

Na coluna Configurar agendas, clique em + para a política que deseja configurar.

c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e clique em **OK**.

Onde, policy_name é o nome da política selecionada.

As programações configuradas são listadas na coluna **programações aplicadas**.

As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas 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 **Finish**.

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 Administrador da infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estão em andamento.

As instalações de plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento, pois 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 do sistema de armazenamento devem ser exclusivos.

O SnapCenter não é compatível com vários sistemas de storage com o mesmo nome em clusters diferentes. Cada sistema de storage com suporte do SnapCenter deve ter um nome exclusivo e um endereço IP de 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 servidor SnapCenter.

```
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:

   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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Faça backup do MySQL

Se um recurso ainda não fizer parte de qualquer 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 uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.
- Para a operação de backup baseada em cópia Snapshot, certifique-se de que todos os bancos de dados do locatário estejam válidos e ativos.
- Para comandos pré e POST para operações quiesce, Snapshot e unquiesce, você deve verificar se os comandos existem na lista de comandos disponível no host plug-in dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização padrão no host Linux: */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*

Se os comandos não existirem na lista de comandos, a operação falhará.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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, em seguida, selecione o nome do host e o tipo de recurso para filtrar os recursos. Em seguida, pode selecionar para fechar o painel de filtro.
3. Selecione o recurso que você deseja fazer backup.
4. Na página recurso, selecione **Use o formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.
5. Na página Configurações do aplicativo, faça o seguinte:
   - Selecione a seta **backups** para definir opções adicionais de backup:

     Ative o backup do grupo de consistência, se necessário, e execute as seguintes tarefas:

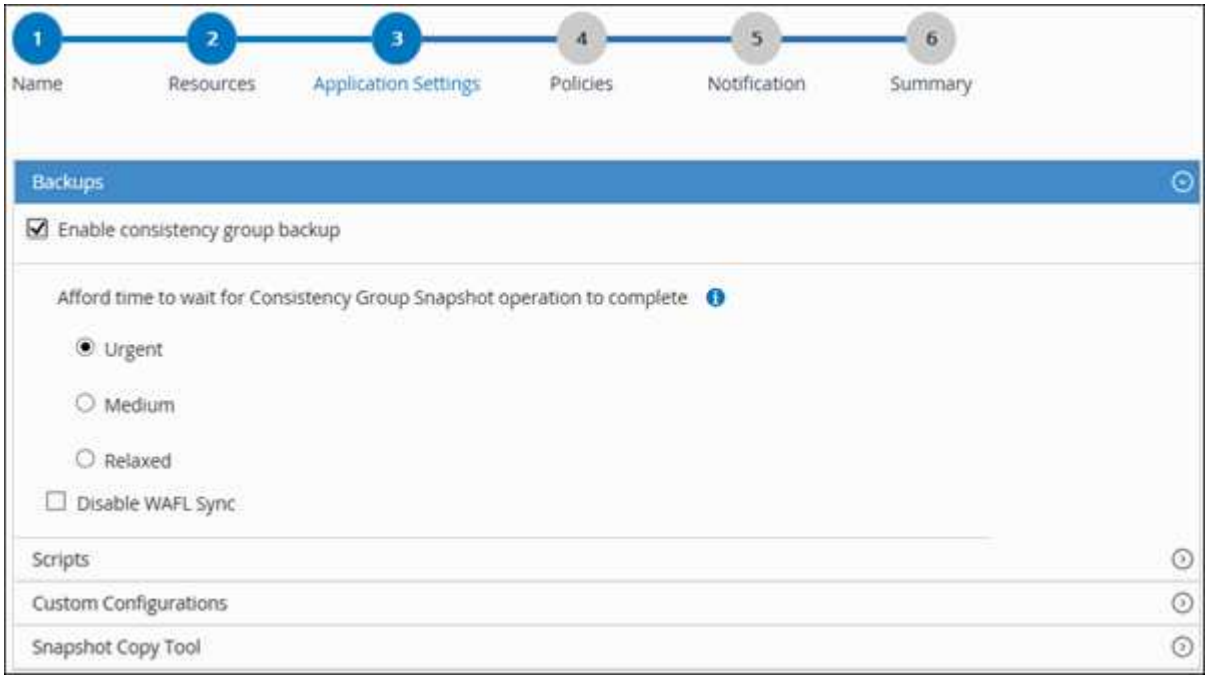
Para este campo…	Faça isso…
Tenha tempo para esperar a conclusão da operação "Consistency Group Snapshot"	Selecione **urgente**, **Médio** ou **relaxado** para especificar o tempo de espera para que a operação Snapshot termine. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL.

   - Selecione a seta **Scripts** para executar comandos pré e POST para operações quiesce, Snapshot e unquiesce.

     Você também pode executar pré-comandos antes de sair da operação de backup. Os Prescripts e postscripts são executados no servidor SnapCenter.
   - Selecione a seta **Custom Configurations (Configurações personalizadas) e, em seguida, insira os pares de valores personalizados necessários para todos os trabalhos que usam esse recurso.
   - Selecione a seta **Snapshot Copy Tool** para selecionar a ferramenta para criar instantâneos:

Se você quiser…	Então…
SnapCenter para criar um Snapshot no nível de storage	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 instantâneo	Selecione **SnapCenter com consistência do sistema de arquivos**.
Para inserir o comando para criar uma captura Instantânea	Selecione **Other** e, em seguida, digite o comando para criar uma captura Instantânea.



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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Selecione + * * na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e selecione **OK**.

      policy_name é o nome da política selecionada.

   As programações configuradas são listadas na coluna agendas aplicadas.

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 **Finish**.

   A página de topologia de recursos é exibida.

9. Selecione **fazer uma cópia de segurança 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. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.
    - Nas configurações do MetroCluster, o SnapCenter pode não ser capaz de detetar uma relação de proteção após um failover.

      Para obter informações, consulte: "Não é possível detetar a relação SnapMirror ou SnapVault após o failover do MetroCluster"

    - Se você estiver fazendo backup de dados de aplicativos em VMDKs e o tamanho de heap Java para o plug-in SnapCenter para VMware vSphere não for grande o suficiente, o backup pode 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 servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

   ```
   Open-SmConnection  -SMSbaseurl
   https:\\snapctr.demo.netapp.com:8146\
   ```

   É apresentado o aviso de nome de utilizador e palavra-passe.

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 da tarefa (em execução, concluída ou com falha) usando o cmdlet Get-smJobSummaryReport.

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. Monitore os detalhes da tarefa de backup, como ID do backup, nome do backup para executar a operação de restauração ou clone 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*. Em alternativa, pode também consultar o "Guia de referência de 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 uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, 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 uma programação configurada, os backups ocorrerão automaticamente de acordo com a programação.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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 selecionando a tag. Em seguida, pode 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. Monitorize 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. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado correspondente das operações:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- 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 a que apenas as operações de cópia de segurança sejam listadas.
b. Especifique as datas de início e fim.
c. Na lista suspensa **Type**, selecione **Backup**.
d. Na lista suspensa **Status**, selecione o status da cópia de segurança.
e. Clique em **Apply** para ver as operações concluídas com êxito.

4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.

Embora o status do trabalho de backup seja exibido , quando você clica nos detalhes do trabalho, você pode ver que algumas das tarefas secundárias da operação de backup ainda estão em andamento ou marcadas com sinais de aviso.

5. Na página Detalhes da tarefa, clique em **Exibir logs**.

O botão **View logs** exibe os logs detalhados para a operação selecionada.

Monitore operações de proteção de dados em instâncias do MySQL no painel atividade

O painel atividade exibe as cinco operações mais recentes executadas. O painel atividade também é exibido quando a operação foi iniciada e o status da operação.

O painel atividade exibe informações sobre operações de backup, restauração, clone e backup agendadas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 da tarefa**.

Cancelar operações de backup para MySQL

Você pode cancelar as operações de backup que estão na fila.

O que você vai precisar

- Você deve estar logado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de cópia de segurança em execução.
- Você pode usar os comandos GUI, cmdlets do SnapCenter ou CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** está desativado 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 em fila de outros membros enquanto usa essa função.

Passos

1. Execute uma das seguintes ações:

A partir 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 da atividade	a. Depois de iniciar a operação de backup, clique em no painel atividade para exibir as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

A operação é cancelada e o recurso é revertido para o estado anterior.

Veja backups e clones do MySQL na página topologia

Ao se preparar para fazer backup ou clonar um recurso, talvez seja útil exibir uma representação gráfica de todos os backups e clones no storage primário e secundário.

Sobre esta tarefa

Você pode revisar os ícones a seguir na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no storage primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups e clones disponíveis no storage primário.
- Exibe o número de backups e clones espelhados no storage secundário usando a tecnologia SnapMirror.
- Exibe o número de backups e clones replicados no storage secundário usando a tecnologia SnapVault.

O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou backups 6 usando uma política para reter apenas 4 backups, o número de backups exibidos é 6.

Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

Na página topologia, você pode ver todos os backups e clones disponíveis para o grupo de recursos ou

recursos selecionado. Você pode visualizar os detalhes desses backups e clones e, em seguida, selecioná-los para executar operações de proteção de dados.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o recurso ou o 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 de 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 baseados em cópia Snapshot.

   Clicar no botão **Refresh** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clique no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Um horário semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo é espalhado por vários volumes, o tempo de expiração do SnapLock para o backup será o tempo de expiração do SnapLock mais longo definido para um snapshot em um volume. O tempo de expiração mais longo do SnapLock é recuperado do ONTAP.

   Após o backup sob demanda, clicando no botão **Refresh** atualiza os detalhes do backup ou clone.

5. No modo de 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 um 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 estão no armazenamento secundário.

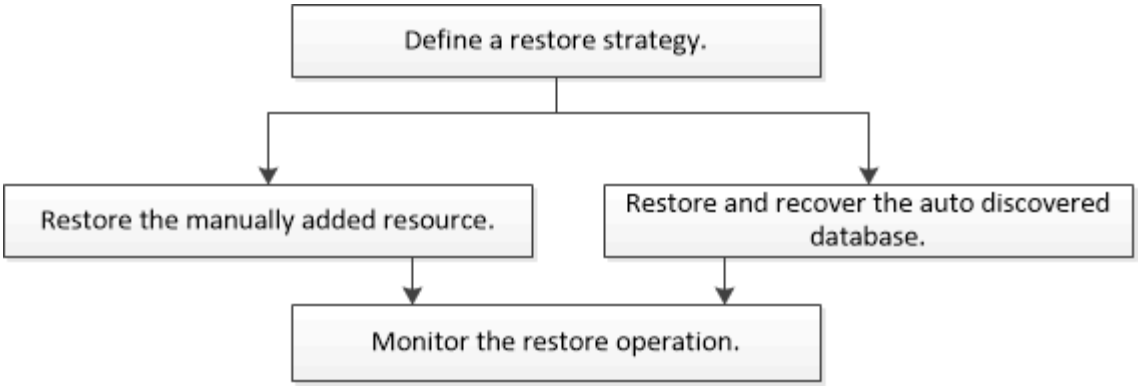
7. Se quiser excluir um clone, selecione-o na tabela e clique em .
8. Se quiser dividir um clone, selecione-o na tabela e clique em .

Restaure o MySQL

Restaure o fluxo de trabalho

O fluxo de trabalho de restauração e recuperação inclui Planejamento, execução das 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 clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre cmdlets do PowerShell.

"Guia de referência de cmdlet do software SnapCenter".

Restaure e recupere um backup de recursos 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 dos grupos de recursos ou recursos.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos pré-restauração, pós restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização 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 versão anterior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com o tipo, host, grupos de recursos e políticas associados e status.

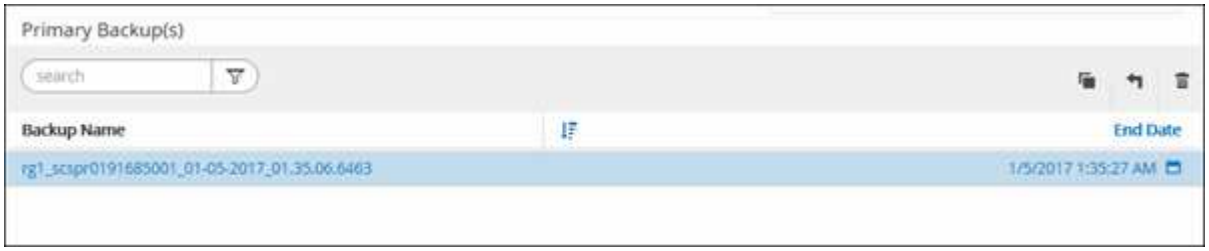
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, ""não protegido"" é exibido na coluna Estado geral. Isso pode significar que o recurso não está protegido ou que o recurso foi protegido 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 do recurso é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Na tabela de backup principal, selecione o backup do qual você deseja restaurar e clique em * * .



6. Na página Restaurar escopo, selecione **recurso completo**.

   a. Se você selecionar **Complete Resource**, todos os volumes de dados configurados do banco de dados MySQL serão restaurados.

      Se o recurso contiver volumes ou qtrees, os instantâneos obtidos 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.

      Pode selecionar vários LUNs.

      Se você selecionar **All**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.

7. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar 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 a execução de 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 **Finish**.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 29th 2015 de janeiro a 3rd 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 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Restaure e recupere 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 dos grupos de recursos ou recursos.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o recurso ou grupo de recursos que deseja restaurar.
- Para comandos pré-restauração, pós restauração, montagem e desmontagem, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter*

Plug-in Creator/etc/allowed_commands.config

- Localização 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 descoberta automática, a restauração é suportada com SFSR.
- Recuperação automática pontual e atualizada não é suportada.
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos snapshots do SnapLock Vault como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com o tipo, host, grupos de recursos e políticas associados e status.

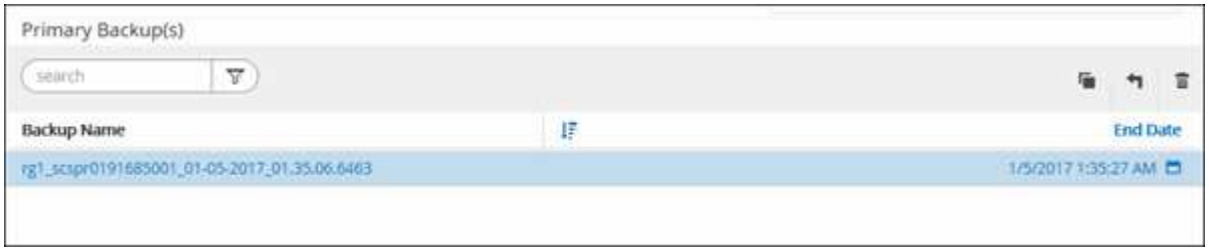
   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

   Se o recurso não estiver protegido, ""não protegido"" é exibido na coluna Estado geral. Isso pode significar que o recurso não está protegido ou que o recurso foi protegido 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 do recurso é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Na tabela de backup principal, selecione o backup do qual você deseja restaurar e clique em * * .



6. Na página Restaurar escopo, selecione **recurso completo** para restaurar os volumes de dados configurados do banco de dados MySQL.
7. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar 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 a execução de 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 **Finish**.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Restaure recursos usando cmdlets do PowerShell

A restauração de um backup de recurso inclui iniciar uma sessão de conexão com o servidor SnapCenter, listar os backups e recuperar informações de backup e 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 servidor SnapCenter 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 29th 2015 de janeiro a 3rd 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 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Monitorar operações de restauração do MySQL

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um 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 executar.

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso

- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Restore**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Clonar backups de recursos MySQL

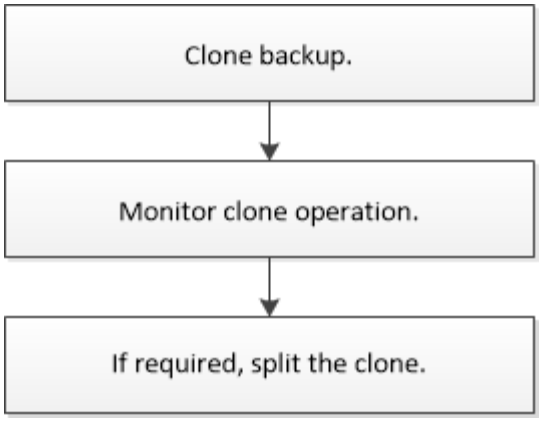
Fluxo de trabalho clone

O fluxo de trabalho do clone inclui a execução da operação de clone e o monitoramento da 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 de aplicativos
  - 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 clone:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clone. A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm informações detalhadas sobre cmdlets do PowerShell.

Clonar um backup MySQL

Você pode usar o SnapCenter para clonar um backup. Você pode clonar 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 storage (SVM).
- Para comandos pré-clone ou pós-clone, você deve verificar se os comandos existem na lista de comandos disponível no host do plug-in a partir dos seguintes caminhos:
  - Localização padrão no host do Windows: *C: Arquivos de programas/NetApp/SnapCenter/SnapCenter Plug-in Creator/etc/allowed_commands.config*
  - Localização 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 do MySQL 5,7, você deve definir IGNORE_MYSQLX_PORT como true (por padrão false) no arquivo MySQL.

Sobre esta tarefa

- Você não pode proteger as instâncias clonadas do MySQL.
- Para obter informações sobre limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .
- Para o ONTAP 9.12,1 e versão anterior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com informações como tipo, host, grupos e políticas de recursos associados e status.

3. Selecione o grupo de recursos ou recursos.

   Você deve selecionar um recurso se selecionar um grupo de recursos.

   A página de topologia do grupo de recursos ou recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Selecione o backup de dados na 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 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. Digite os comandos para pré-clone ou pós-clone que devem ser executados antes ou depois da operação clone, respetivamente.
      - Comando pre clone: Exclua bancos de dados existentes com o mesmo nome
      - Comando Post clone: Verifique um banco de dados ou inicie um banco de dados.
   b. Digite o comando mount para montar um sistema de arquivos em um host.

      Monte o comando 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 **Finish**.
10. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 clone 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 clone a partir de um backup existente e especifique os endereços IP de exportação NFS nos quais os volumes clonados são 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 clone.

4. Verifique se os backups foram clonados com sucesso usando o cmdlet Get-SmCloneReport para exibir os detalhes da tarefa clone.

   Você pode exibir 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 clone do MySQL

Você pode monitorar o andamento das operações de clone do SnapCenter usando a página tarefas. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.

3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista para que apenas operações de clone sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Divida um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone que é dividido torna-se independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clones em um clone intermediário.

  Por exemplo, depois de criar clone1 a partir de um backup de banco de dados, você pode criar um backup de clone1 e clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e não é possível executar a operação de divisão de clones no clone1. No entanto, você pode executar a operação de divisão de clones no clone2.

  Depois de dividir clone2, você pode executar a operação de divisão de clones no clone1 porque clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e as tarefas de clone do clone são excluídas.
- Para obter informações sobre limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .
- Certifique-se de que o volume ou o agregado no sistema de storage esteja on-line.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página **recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicativos 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 do recurso é exibida.

4. No modo de 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 deve ser dividido e o espaço necessário disponível no agregado

e clique em **Iniciar**.

6. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

   A operação de divisão de clones deixa de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clones e tentar novamente a operação de divisão de clones.

   Se você quiser um tempo de enquete mais longo 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 que o SMCore busque o status da operação de divisão de clones. O valor é em milissegundos e o valor padrão é de 5 minutos.

   Por exemplo:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   A operação de inicialização dividida de clone falhará se o backup, a restauração ou outra divisão de clones estiver em andamento. Você deve reiniciar a operação de divisão de clones somente depois que as operações em execução estiverem concluídas.

Informações relacionadas

"O clone ou a verificação do SnapCenter falha com o agregado não existe"

Excluir ou dividir clones do banco de dados MySQL após a atualização do SnapCenter

Após a atualização para o SnapCenter 4,3, você não verá mais os clones. Você pode excluir o clone ou dividir os clones da página topologia do recurso a partir do qual os clones foram criados.

Sobre esta tarefa

Se você quiser localizar o espaço físico 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-sprotectresource.
4. Selecione o recurso pai na página recursos.

   A página de topologia do recurso é exibida.

5. Na visualização Gerenciar cópias, selecione os clones nos sistemas de storage primário ou secundário (espelhado ou replicado).
6. Selecione os clones e clique para excluir clones ou clique para dividir os clones.
7. Clique em **OK**.

Proteja aplicativos usando plug-ins compatíveis com NetApp

Plug-ins compatíveis com NetApp

Visão geral dos plug-ins compatíveis com NetApp

Você pode usar os plug-ins compatíveis com o NetApp, como MongoDB, ORASCPM (aplicações Oracle), SAP ASE, SAP MaxDB e plug-in de storage para aplicativos que você usa e depois usa o SnapCenter para fazer backup, restauração ou clonagem desses aplicativos. Seus plug-ins compatíveis com NetApp atuam como componentes do lado do host do software NetApp SnapCenter, permitindo a proteção de dados com reconhecimento de aplicações e o gerenciamento de recursos.

Quando os plug-ins compatíveis com NetApp estão instalados, você pode usar a tecnologia SnapCenter com 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 disco para disco. Os plug-ins compatíveis com NetApp podem ser usados em ambientes Windows e Linux.

SnapCenterCLI não suporta comandos de plug-ins suportados pelo NetApp.

Você pode instalar os plug-ins suportados pelo NetApp na página Adicionar Host. "Adicione hosts e instale pacotes plug-in em hosts remotos."

O que você pode fazer com os plug-ins compatíveis com o NetApp

Você pode usar os plug-ins compatíveis com NetApp, como MongoDB, ORASCPM, aplicações Oracle, SAP ASE, SAP MaxDB e plug-in de storage para operações de proteção de dados.

- Adicione recursos como bancos de dados, instâncias, documentos ou espaços de tabela.
- Criar backups.
- Restauração a partir de backups.
- Backups de clones.
- Agendar operações de backup.
- Monitore operações de backup, restauração e clone.
- Exibir relatórios para operações de backup, restauração e clone.

Você pode usar os plug-ins compatíveis com NetApp para operações de proteção de dados.

- Tire snapshots de grupos de consistência dos volumes de storage nos clusters do ONTAP.
- Faça backup de aplicativos personalizados usando a estrutura de script pré e pós integrada

  Você pode fazer backup do volume ONTAP, LUN ou Qtree.

- Atualize os snapshots feitos no primário para um secundário ONTAP, aproveitando a relação de replicação

existente (SnapVault/SnapMirror/replicação unificada) usando a política SnapCenter

O ONTAP primário e o secundário podem ser ONTAP FAS, AFF, All SAN Array (ASA), Select ou Cloud ONTAP.

- Recupere o volume, LUN ou arquivos completos do ONTAP.

  Você deve fornecer o caminho do arquivo respetivo manualmente, pois os recursos de pesquisa ou indexação não estão incorporados ao produto.

  A restauração de Qtree ou diretório não é suportada, mas você pode clonar e exportar apenas o Qtree se o escopo de backup estiver definido em um nível Qtree.

Recursos de plug-ins compatíveis com NetApp

O SnapCenter se integra à aplicação plug-in e às tecnologias NetApp no sistema de storage. Para trabalhar com plug-ins compatíveis com NetApp, como MongoDB, ORASCPM (aplicações Oracle), SAP ASE, SAP MaxDB e plug-in de storage, você usa a interface gráfica de usuário do SnapCenter.

- * Interface gráfica unificada do usuário*

  A interface do SnapCenter fornece padronização e consistência em plug-ins e ambientes. A interface do SnapCenter permite concluir operações consistentes de backup, restauração, recuperação e clone em plug-ins, usar relatórios centralizados, usar visualizações de dashboard rápidas, configurar controle de acesso baseado em funções (RBAC) e monitorar tarefas em todos os plug-ins.

- * Administração central automatizada*

  Você pode agendar operações de backup, configurar a retenção de backup baseada em política e executar operações de restauração. Você também pode monitorar proativamente seu ambiente configurando o SnapCenter para enviar alertas por e-mail.

- **Tecnologia NetApp Snapshot sem interrupções**

  O SnapCenter usa a tecnologia Snapshot do NetApp com os plug-ins compatíveis com o NetApp para fazer backup de recursos. Os snapshots consomem espaço mínimo de storage.

Os plug-ins compatíveis com NetApp também oferecem os seguintes benefícios:

- Suporte a fluxos de trabalho de backup, restauração e clone
- Delegação de funções centralizada e segurança compatível com RBAC

  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 uso eficiente de espaço e pontuais para teste ou extração de dados usando a tecnologia NetApp FlexClone

  É necessária uma licença FlexClone no sistema de storage onde você deseja criar o clone.

- Suporte ao recurso Snapshot do grupo de consistência (CG) do ONTAP como parte da criação de backups.

- Funcionalidade de executar vários backups simultaneamente em vários hosts de recursos

  Em uma única operação, os snapshots são consolidados quando os recursos em um único host compartilham o mesmo volume.

- Capacidade de criar Snapshot usando comandos externos.
- Capacidade de criar snapshots consistentes no sistema de arquivos em ambientes Windows.

Tipos de storage compatíveis com plug-ins compatíveis com 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 storage antes de instalar os plug-ins compatíveis com NetApp.

Máquina	Tipo de armazenamento
Montagens físicas e diretas NFS nos hosts de VM (VMDKs e RDM LUNs não são compatíveis.)	LUNs conectados a FC
Montagens físicas e diretas NFS nos hosts de VM (VMDKs e RDM LUNs não são compatíveis.)	LUNs ligados ao iSCSI
Montagens físicas e diretas NFS nos hosts de VM (VMDKs e RDM LUNs não são compatíveis.)	Volumes conectados a NFS
VMware ESXi	Armazenamentos de dados da VVol em NFS e SAN O armazenamento de dados da VVol só pode ser provisionado com as Ferramentas do ONTAP para o VMware vSphere.

Mínimo de ONTAP Privileges necessário para o plug-in compatível com NetApp

Os ONTAP Privileges mínimos necessários variam de acordo com os plug-ins do SnapCenter que você está usando para proteção de dados.

- Comandos All-Access: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
  - event generate-AutoSupport-log
  - mostra o histórico de trabalhos
  - paragem do trabalho
  - show de atributo lun
  - lun criar
  - eliminação lun
  - geometria lun
  - lun igrop add
  - lun igrop criar

- eliminação do agrupamento lun
- mudar o nome do grupo lun
- show de grupos de lun
- nós complementares de mapeamento de lun
- mapeamento lun criar
- eliminação do mapeamento lun
- mapeamento lun remove-reporting-nonos
- mostra de mapeamento lun
- modificação de lun
- movimentação de lun no volume
- lun offline
- lun online
- redimensionar lun
- série lun
- mostra lun
- interface de rede
- regra adicional de política do SnapMirror
- regra de modificação de política do SnapMirror
- regra de remoção da política do SnapMirror
- SnapMirror policy show
- restauração de SnapMirror
- SnapMirror show
- SnapMirror show-history
- atualização do SnapMirror
- SnapMirror update-ls-set
- SnapMirror lista-destinos
- versão
- clone de volume criar
- show de clone de volume
- início da divisão do clone de volume
- paragem dividida clone volume
- criar volume
- destruição de volume
- clone de arquivo de volume criar
- show-disk-use do arquivo de volume
- volume off-line
- volume online

    - modificação do volume
    - criar qtree de volume
    - eliminação de qtree de volume
    - modificação de qtree de volume
    - apresentação de qtree de volume
    - restrição de volume
    - apresentação do volume
    - criar instantâneo de volume
    - eliminar instantâneo do volume
    - modificação do instantâneo do volume
    - mudar o nome do instantâneo do volume
    - restauração de snapshot de volume
    - restauração de arquivo de snapshot de volume
    - apresentação de instantâneo do volume
    - desmontar o volume
    - svm cifs
    - compartilhamento cifs de svm criar
    - exclusão de compartilhamento cifs de svm
    - apresentação do shadowcopy cifs de svm
    - exibição de compartilhamento cifs de svm
    - mostra cifs de svm
    - criação de política de exportação de svm
    - exclusão da política de exportação do svm
    - regra de política de exportação de svm criar
    - a regra de política de exportação do svm é exibida
    - exibição da política de exportação do svm
    - apresentação da ligação iscsi de svm
    - mostra o svm
- Comandos somente leitura: Privileges mínimo necessário para o ONTAP 8.3.0 e posterior
    - interface de rede

Preparar sistemas de storage para a replicação do SnapMirror e do SnapVault para plug-ins compatíveis com NetApp

Você pode usar um plug-in do 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 disco a disco para conformidade com os padrões e outros fins relacionados à governança. Antes de executar essas tarefas, você deve configurar uma relação de proteção de dados entre os volumes de

origem e destino e inicializar a relação.

O SnapCenter executa as atualizações para o SnapMirror e o SnapVault após concluir a operação de captura instantânea. As atualizações SnapMirror e SnapVault são executadas como parte da tarefa SnapCenter; não crie uma agenda ONTAP separada.

Se você estiver vindo para o SnapCenter de um produto NetApp SnapManager e estiver satisfeito com as relações de proteção de dados que configurou, ignore esta seção.

Uma relação de proteção de dados replica dados no storage primário (o volume de origem) para o storage secundário (o volume de destino). Ao inicializar a relação, o ONTAP transfere os blocos de dados referenciados no volume de origem para o volume de destino.

O SnapCenter não suporta relações em cascata entre volumes SnapMirror e SnapVault (**Primary** > **Mirror** > **Vault**). Você deve usar relacionamentos de fanout.

O SnapCenter oferece suporte ao gerenciamento de relacionamentos SnapMirror flexíveis de versão. Para obter detalhes sobre relacionamentos SnapMirror flexíveis de versão e como configurá-los, consulte "Documentação do ONTAP".

Defina uma estratégia de backup

Definir uma estratégia de backup antes de criar seus trabalhos de backup garante que você tenha os backups necessários para restaurar ou clonar seus recursos com êxito. Seu contrato de nível de serviço (SLA), objetivo de tempo de recuperação (rto) e objetivo do ponto de restauração (RPO) determinam em grande parte a sua estratégia de backup.

Sobre esta tarefa

Um SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. Rto é o momento em que um processo de negócios deve ser restaurado após uma interrupção no serviço. O RPO define a estratégia para a era dos arquivos que precisam 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 de seus recursos.
2. Decida quantos trabalhos de cópia de segurança necessita.
3. Decida como nomear seus backups.
4. Decida se você deseja Snapshots de Grupo de consistência e decida as opções apropriadas para excluir Snapshots de Grupo de consistência.
5. Decida se você deseja usar a tecnologia NetApp SnapMirror para replicação ou a tecnologia NetApp SnapVault para retenção a longo prazo.
6. Determine o período de retenção dos snapshots no sistema de storage de origem e no destino do SnapMirror.
7. Determine se deseja executar quaisquer comandos antes ou depois da operação de backup e forneça um prescritor ou postscript.

Estratégia de backup para plug-ins compatíveis com NetApp

Programações de backup de recursos de plug-in compatíveis com NetApp

O fator mais crítico na determinação de um agendamento de backup é a taxa de alteração do recurso. Quanto mais você fizer backup de seus recursos, menos Registros de arquivamento que o SnapCenter precisa usar para restaurar, o que pode resultar em operações de restauração mais rápidas.

Você pode fazer backup de um recurso muito usado a cada hora, enquanto você pode fazer backup de um recurso raramente usado uma vez por dia. Outros fatores incluem a importância do recurso para a sua organização, seu contrato de nível de serviço (SLA) e seu objetivo do ponto de restauração (RPO).

O SLA define o nível de serviço esperado e aborda muitos problemas relacionados ao serviço, incluindo a disponibilidade e o desempenho do serviço. O RPO define a estratégia para a era dos arquivos que precisam 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.

Os programas de backup têm duas partes, como segue:

- Frequência de backup

  A frequência de backup (com que frequência os backups devem ser executados), 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 hora, dia, semanal ou mensal. Você pode acessar políticas na GUI do SnapCenter clicando em **Configurações** > **políticas**.

- Fazer backup de programações

  As programações 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 que tenha uma política configurada para backups semanais, poderá configurar a programação para fazer backup todas as quintas-feiras às 10:00 horas. Você poderá acessar programações de grupos de recursos na GUI do SnapCenter clicando em **Resources**, selecionando o plug-in apropriado e clicando em **Exibir** > **Grupo de recursos**.

Número de trabalhos de cópia de segurança necessários

Os fatores que determinam o número de tarefas de backup de que você precisa 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 geralmente depende do número de volumes nos quais você colocou seus recursos. Por exemplo, se você colocou um grupo de pequenos recursos em um volume e um recurso grande em outro volume, poderá criar uma tarefa de backup para os pequenos recursos e uma tarefa de backup para o recurso grande.

Tipos de estratégias de restauração compatíveis com recursos de plug-in compatíveis com NetApp adicionados manualmente

Você deve definir uma estratégia antes de executar operações de restauração com êxito usando o SnapCenter. Existem dois tipos de estratégias de restauração para recursos de

plug-in compatíveis com NetApp adicionados manualmente.

Não é possível recuperar recursos de plug-in suportados pelo 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 instantâneos obtidos 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.

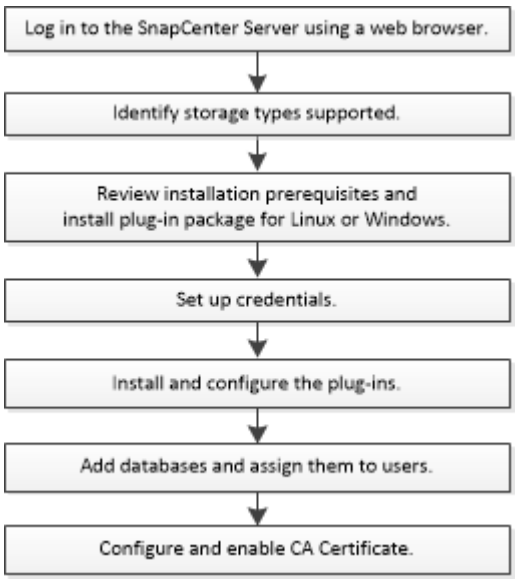
Restauração no nível do arquivo

- 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-in compatíveis com o NetApp.



Pré-requisitos para adicionar hosts e instalar o pacote Plug-ins para Windows, Linux ou AIX

Antes de adicionar um host e instalar os pacotes de plug-ins, você deve completar todos os requisitos. Os plug-ins compatíveis com NetApp são compatíveis com ambientes Windows, Linux e AIX.

Os aplicativos de armazenamento e Oracle são compatíveis com AIX.

- Você deve ter instalado o Java 11 em seu host Linux, Windows ou AIX.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host.
- Os plug-ins compatíveis com o NetApp, como MongoDB, ORASCPM, aplicativos Oracle, 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 executada.

Geral

Se estiver a utilizar iSCSI, o serviço iSCSI deverá estar em execução.

Hosts do Windows

- Você deve ter um usuário de domínio com Privileges de administrador local com permissões de login local no host remoto.
- Se você gerenciar nós de cluster no SnapCenter, precisará ter um usuário com Privileges administrativo para todos os nós do cluster.
- Você deve escolher manualmente o plug-in do SnapCenter para Microsoft Windows.

Hosts Linux e AIX

Os aplicativos de armazenamento e Oracle são compatíveis com 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 em seu host Linux.

  Se você estiver usando o Windows Server 2019 ou o Windows Server 2016 para o host do servidor SnapCenter, você deve instalar o Java 11. A ferramenta de Matriz de interoperabilidade (IMT) contém as informações mais recentes sobre os requisitos.

  "Downloads Java para todos os sistemas operacionais"

  "Ferramenta de Matriz de interoperabilidade do NetApp"

- Você deve configurar o sudo Privileges 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 que está a utilizar 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 !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**, que está localizado em:

- Se o servidor SnapCenter estiver instalado no host do Windows, o SnapCenter NetApp não será instalado no sistema operacional Windows.
- */opt/NetApp/SnapCenter/SnapManagerWeb/Repository/SC_UNIX_plugins_checksum.txt* se o servidor SnapCenter estiver instalado no host Linux.

> O exemplo deve ser usado apenas como referência para criar seus próprios dados.

Requisitos de anfitrião do AIX

Você deve garantir que o host atenda aos requisitos antes de instalar o pacote de plug-ins do SnapCenter para AIX.

> Os aplicativos de armazenamento e Oracle são compatíveis com AIX.

> O plug-in do SnapCenter para UNIX, que faz parte do pacote de plug-ins do SnapCenter para AIX, não suporta grupos de volume simultâneos.

Item	Requisitos
Sistemas operacionais	AIX 7,1 ou posterior
RAM mínima para o plug-in SnapCenter no host	4 GB

Item	Requisitos
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto.

Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Configure sudo Privileges para usuários não-root para host AIX

O SnapCenter 4,4 e posterior permite que um usuário não root instale o pacote de plug-ins do SnapCenter para AIX e inicie o processo de plug-in. Os processos de plug-in serão executados como um usuário não-root eficaz. Você deve configurar o sudo Privileges 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 de código de autenticação de mensagem: Macs hmac-SHA2-256 e MACs hmac-SHA2-512.

  Reinicie o serviço sshd depois de 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 o sudo Privileges para que o usuário não-root forneça acesso aos seguintes caminhos:

- /Home/*AIX_USER*/.SC_NetApp/SnapCenter_aix_host_plugin.bsx
- /Custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall
- /Custom_location/NetApp/SnapCenter/spl/bin/spl

Passos

1. Faça 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: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```

Se você estiver tendo uma configuração RAC, juntamente 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**, que está localizado em:

- Se o servidor SnapCenter estiver instalado no host do Windows, o SnapCenter NetApp não será instalado no sistema operacional Windows.
- */opt/NetApp/SnapCenter/SnapManagerWeb/Repository/SC_UNIX_plugins_checksum.txt* se o servidor SnapCenter 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 do 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 do sistema host e requisitos de dimensionamento.

Item	Requisitos
Sistemas operacionais	Microsoft Windows Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	5 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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	• .NET Core começando com a versão 8.0.5 e incluindo todos os patches .NET 8 subsequentes • PowerShell Core 7.4.2 • Java 11 Oracle Java e OpenJDK Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp". Para obter informações específicas de solução de problemas .NET, consulte "A atualização ou instalação do SnapCenter falha para sistemas legados que não têm conetividade com a Internet."

Requisitos de host para instalar o pacote de plug-ins do 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.

Os aplicativos de armazenamento e Oracle são compatíveis com AIX.

Item	Requisitos
Sistemas operacionais	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
RAM mínima para o plug-in SnapCenter no host	1 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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 ou OpenJDK Se você atualizou O JAVA para a versão mais recente, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto.

Para obter as informações mais recentes sobre versões suportadas, consulte a. "Ferramenta de Matriz de interoperabilidade do 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 raiz ou para um usuário não-root que tenha sudo Privileges para instalar e iniciar o processo de plug-in.

  Prática recomendada: embora você tenha permissão para criar credenciais para Linux após implantar hosts e instalar plug-ins, a prática recomendada é criar credenciais após adicionar SVMs, antes de implantar hosts e instalar plug-ins.

- Hosts do Windows

  Você deve configurar as credenciais do Windows antes de instalar os plug-ins.

  Você deve configurar as credenciais com o Privileges de administrador, incluindo direitos de administrador no host remoto.

- Aplicações de plug-ins compatíveis com 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 pode definir as credenciais como **Nenhuma**.

Sobre esta tarefa

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

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Clique em **novo**.
4. Na página **Credential**, especifique as informações necessárias para configurar credenciais:

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para as credenciais.
Nome de utilizador	Introduza o nome de utilizador e a palavra-passe a utilizar para a 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 no qual você está instalando o plug-in do SnapCenter. Formatos válidos para o campo Nome de usuário são: ◦ *NetBIOS_username* ◦ *Domain FQDN_username* • Administrador local (apenas para grupos de trabalho) Para sistemas que pertencem a um grupo de trabalho, especifique o administrador local incorporado no sistema no qual você está instalando o plug-in SnapCenter. Você pode especificar uma conta de usuário local que pertence ao grupo de administradores locais se a conta de usuário tiver Privileges elevado ou o recurso de controle de acesso do usuário estiver desativado no sistema host. O formato válido para o campo Nome de usuário é: *Nome de usuário*
Palavra-passe	Introduza a palavra-passe utilizada para autenticação.
Tipo de autenticação	Selecione o tipo de autenticação que pretende utilizar.

Para este campo…	Faça isso…
Use sudo Privileges	Marque a caixa de seleção **Use sudo Privileges** se estiver criando credenciais para um usuário que não seja root. Aplicável apenas a usuários 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.

Configure o gMSA no Windows Server 2016 ou posterior

O Windows Server 2016 ou posterior permite criar uma conta de serviço gerenciado de grupo (gMSA) que fornece gerenciamento automatizado de senha de conta de serviço a partir de uma conta de domínio gerenciado.

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 é um membro do domínio.

Passos

1. Crie uma chave raiz KDS para gerar senhas exclusivas para cada objeto em seu gMSA.
2. Para cada domínio, execute o seguinte comando do 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,…>
.. Execute `Get-ADServiceAccount` o comando para verificar a conta de
serviço.
```

4. Configure o gMSA em seus hosts:

a. Ative o módulo do ative Directory para Windows PowerShell no host onde você deseja usar a conta gMSA.

   Para fazer isso, execute o seguinte comando do 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 o host.

   b. Instale o gMSA em seu host executando o seguinte comando a partir do prompt de comando do PowerShell: `Install-AdServiceAccount <gMSA>`

   c. Verifique sua conta gMSA executando o seguinte comando: `Test-AdServiceAccount <gMSA>`

5. Atribua o Privileges administrativo ao gMSA configurado no host.
6. Adicione o host do Windows especificando a conta gMSA configurada no servidor SnapCenter.

   O servidor SnapCenter 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.

Instale os plug-ins suportados pelo NetApp

Adicione hosts e instale pacotes plug-in em hosts remotos

Você deve usar a página SnapCenter Adicionar host 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 as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Você deve garantir que o serviço de enfileiramento de mensagens esteja em execução.

- Se você estiver usando a conta de serviço gerenciado de grupo (gMSA), você deve configurar o gMSA com Privileges administrativo.

  "Configure a conta de serviço gerenciado de grupo no Windows Server 2016 ou posterior para aplicativos personalizados"

- Para o host do Windows, você deve garantir que você selecione o plug-in do SnapCenter para Windows.

Sobre esta tarefa

- Não é possível adicionar um servidor SnapCenter como um host plug-in a outro servidor SnapCenter.
- 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 guia **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 compatíveis com NetApp podem ser usados em ambientes Windows, Linux e AIX. Os aplicativos de armazenamento e Oracle são compatíveis com AIX.

Para este campo…	Faça isso…
Nome do host	Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no 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.
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 exibir 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 **Select Plug-ins to Install**, selecione os plug-ins a instalar.

   Você pode instalar os seguintes plug-ins na lista:

   - MongoDB
   - ORASCPM (exibido como aplicativos Oracle)
   - SAP ASE
   - SAP MaxDB
   - Armazenamento

6. (Opcional) Selecione **mais opções** para instalar os outros plug-ins.

Para este campo…	Faça isso…
Porta	Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido 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, você deve especificar a mesma porta. Caso contrário, a operação falha.
Caminho de instalação	Os plug-ins compatíveis com NetApp podem ser instalados em um sistema Windows ou em um sistema Linux. • Para o pacote de plug-ins do 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 do SnapCenter para Linux e o pacote de plug-ins do SnapCenter para AIX, o caminho padrão é `/opt/NetApp/snapcenter`. Opcionalmente, você pode personalizar o caminho.
Ignorar as verificações de pré-instalação	Marque essa caixa de seleção se você já instalou os plug-ins manualmente e não quiser validar se o host atende aos requisitos para instalar o plug-in.

Para este campo…	Faça isso…
Use a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in	Para o host Windows, marque essa caixa de seleção se desejar usar a conta de serviço gerenciado de grupo (gMSA) para executar os serviços de plug-in. Forneça o nome do gMSA no seguinte formato: O gMSA será usado como uma conta de serviço de logon apenas para o serviço SnapCenter Plug-in para Windows.

7. Selecione **Enviar**.

   Se você não tiver selecionado a caixa de seleção **Ignorar pré-verificações**, o host será validado para verificar se o host 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 Java (para plug-ins do Linux) são validados de acordo com os requisitos mínimos. Se os requisitos mínimos não forem cumpridos, são apresentadas mensagens de erro ou de aviso adequadas.

   Se o erro estiver relacionado ao espaço em disco ou à RAM, você poderá 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 deve corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o SnapManager.Web.UI.dll.config, será necessário atualizar o arquivo em ambos os nós e reiniciar o pool de aplicativos do SnapCenter.

   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 **Confirm and Submit**.

   A verificação de impressões digitais é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitorize o progresso da instalação.

   Os arquivos de log específicos da instalação estão localizados em `/custom_location/snapcenter/logs`.

Instale pacotes de plug-in do 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 PowerShell.

Antes de começar

O usuário que adiciona um host deve ter os direitos administrativos no host.

Os aplicativos de armazenamento e Oracle são compatíveis com AIX.

Passos

1. Inicie o PowerShell.
2. No host do servidor SnapCenter, 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*. Em alternativa, pode também consultar o "Guia de referência de 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 compatíveis com NetApp em hosts Linux usando a interface de linha de comando

Você deve instalar os plug-ins compatíveis com o NetApp usando a interface de usuário (UI) do SnapCenter. Se o seu ambiente não permitir a instalação remota do plug-in a partir da IU do SnapCenter, você poderá instalar os plug-ins compatíveis com NetApp no modo console ou no modo silencioso usando a interface de linha de comando (CLI).

Passos

1. Copie o pacote de plug-ins do SnapCenter para o arquivo de instalação do Linux (SnapCenter_linux_host_plugin.bin) de C:/NetApp/SnapCenter para o host onde você deseja instalar os plug-ins suportados pelo NetApp.

   Você pode acessar esse caminho a partir do host onde o servidor SnapCenter 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 SMCore.
   - -DSERVER_IP especifica o endereço IP do servidor SnapCenter.
   - -DSERVER_HTTPS_PORT especifica a porta HTTPS do servidor SnapCenter.
   - -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 servidor SnapCenter 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

5. Faça login no SnapCenter e faça o upload do plug-in compatível com o NetApp a partir da IU ou usando cmdlets do PowerShell.

   Pode carregar o plug-in suportado pelo NetApp a partir da IU consultando "Adicione hosts e instale pacotes plug-in em hosts remotos"a secção.

   A ajuda do cmdlet SnapCenter e as informações de referência do cmdlet contêm mais informações sobre cmdlets do PowerShell.

   "Guia de referência de cmdlet do software SnapCenter".

Monitore o status da instalação de plug-ins compatíveis com o NetApp

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
   a. Clique em **filtro**.
   b. Opcional: Especifique a data de início e fim.

c. No menu suspenso tipo, selecione **Instalação 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 **Visualizar logs**.

Configurar certificado CA

Gerar arquivo CSR do 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 a CSR gerada. O certificado terá uma chave privada associada a ele.

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

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

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

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

Para configurações de cluster, o nome do cluster (FQDN de cluster virtual) e os respetivos nomes de host devem ser mencionados no certificado da CA. O certificado pode ser atualizado preenchendo o campo Nome alternativo (SAN) do assunto antes de adquirir o certificado. Para um certificado Wild card (*.domain.company.com), o certificado conterá todos os nomes de host do domínio implicitamente.

Importar certificados CA

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

Passos

1. Vá para o console de gerenciamento da Microsoft (MMC) e clique em **File** > **Add/Remove Snapin**.
2. Na janela Adicionar ou remover snap-ins, selecione **certificados** e clique em **Adicionar**.
3. Na janela de snap-in certificados, selecione a opção **conta de computador** e clique em **concluir**.
4. Clique em **raiz da consola** > **certificados – computador local** > **autoridades de Certificação raiz fidedignas** > **certificados**.
5. Clique com o botão direito do rato na pasta "autoridades de Certificação de raiz fidedigna" 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 **Yes**, importe a chave privada e clique em **Next**.
Importar formato de ficheiro	Não faça alterações; clique em **seguinte**.
Segurança	Especifique a nova senha a ser usada para o certificado exportado e clique em **Avançar**.
Concluir o Assistente de importação de certificados	Revise o resumo e clique em **Finish** para iniciar a importação.

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

7. Repita o passo 5 para a pasta "Pessoal".

Obtenha a impressão digital do certificado CA

Uma impressão digital de certificado é uma cadeia 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 **thumbprint**.
   d. Copie os carateres 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", depois de remover os espaços, será: "A909502d82ae41433e6f83886b00d4277a32a7b".

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.

Configure o certificado CA com os serviços de plug-in do host do Windows

Você deve configurar o certificado CA com os serviços de plug-in host do Windows para ativar o certificado digital instalado.

Execute as etapas a seguir no servidor SnapCenter e em todos os hosts de plug-in em que os certificados de CA já estão implantados.

Passos

1. Remova a vinculação de certificado existente com a porta padrão SMCore 8145, 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"
   ```

Configure o certificado CA para o serviço de plug-ins compatíveis com 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. Altere a senha do keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Altere a senha para 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 depois de 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. Liste 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 de CA raiz e, em seguida, os certificados de CA intermediários.

Configurar o par de chaves assinadas pela CA para plug-in de armazenamento confiável

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. Liste 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. Liste os certificados adicionados no keystore.

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

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da CA para a senha do keystore.

   A senha padrão do keystore 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 espaço ou
carateres 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 com a chave SCC_CERTIFICATE_ALIAS.

8. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o plug-in trust-store.

Configurar a lista de revogação de certificados (CRL) para plug-ins do SnapCenter

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 SnapCenter é 'opt/NetApp/snapcenter/scc/etc/crl'.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo agent.properties contra a chave CRL_PATH.

   Você pode colocar mais de um arquivo CRL neste diretório. Os certificados recebidos serão verificados em relação a cada CRL.

Configure o certificado CA para o serviço de plug-ins compatíveis com o 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 Plug-ins 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. Altere 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 por seu caminho completo.

   C: Arquivos de programas/<jdk_version>/keytool.exe" -storepasswd -keystore keystore.jks

3. Altere a senha para 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*.

4. Reinicie o serviço depois de 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. Liste 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 de CA raiz e, em seguida, os certificados de CA intermediários.

Configurar o par de chaves assinadas pela CA para plug-in de armazenamento confiável

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. Liste 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 -destinkeystore keystore.jks -deststoretype JKS

5. Liste os certificados adicionados no keystore.

   keytool -list -v -keystore keystore.jks

6. Verifique se o keystore contém o alias correspondente ao novo certificado da CA, que foi adicionado ao keystore.
7. Altere a senha da chave privada adicionada para o certificado da 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

8. Configure o nome do alias do certificado CA no arquivo *agent.properties*.

   Atualize este valor com a chave SCC_CERTIFICATE_ALIAS.

9. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o plug-in trust-store.

Configurar a lista de revogação de certificados (CRL) para plug-ins do SnapCenter

Sobre esta tarefa

- Para transferir o ficheiro CRL mais recente para o certificado CA relacionado, "Como atualizar o arquivo de lista de revogação de certificados no certificado da CA do SnapCenter"consulte .
- 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* contra a chave CRL_PATH.
2. Você pode colocar mais de um arquivo CRL neste diretório.

Os certificados recebidos serão verificados em relação a cada CRL.

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet RUN *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando as *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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- * * Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da 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 são concluídas com êxito.

Preparar-se para a proteção de dados

Pré-requisitos para usar os plug-ins suportados pelo NetApp

Antes de usar plug-ins compatíveis com o SnapCenter NetApp, o administrador do SnapCenter deve instalar e configurar o servidor SnapCenter e executar as tarefas de pré-requisito.

- Instalar e configurar o servidor SnapCenter.
- Inicie sessão no servidor SnapCenter.

- Configure o ambiente SnapCenter adicionando conexões do sistema de storage e criando credenciais, se aplicável.
- Adicione hosts e 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, você pode 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 storage NFS na máquina virtual de armazenamento (SVM) para os volumes clonados. Se você quiser ter um endereço IP específico ou restringir a um subconjunto dos 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 a montagem do volume clonado NFS. No entanto, se você quiser especificar um caminho de dados específico (LIF), você deve 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*. Em alternativa, pode também consultar o "Guia de Referência de comandos do software SnapCenter".
- Configure o SnapMirror e o SnapVault, se quiser replicação de backup.
- Certifique-se de que a porta 9090 não seja usada por nenhum outro aplicativo no host.

  A porta 9090 deve ser reservada para uso pelos plug-ins compatíveis com NetApp, além das outras portas exigidas pelo SnapCenter.

Como os recursos, grupos de recursos e políticas são usados para proteger os recursos de plug-in compatíveis com o NetApp

Antes de usar o SnapCenter, é útil entender 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 clone com o SnapCenter.
- Um grupo de recursos do SnapCenter é uma coleção de recursos em um host ou cluster.

  Quando você executa uma operação em um grupo de recursos, executa essa operação nos recursos definidos no grupo de recursos de acordo com a programação especificada 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 programados para recursos únicos e grupos de recursos.

- As políticas especificam a frequência de backup, retenção de cópia, 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 quando você executa um backup sob demanda para um único recurso.

Pense em um grupo de recursos como definindo *o que* você quer proteger e quando você quer protegê-lo em termos de dia e tempo. Pense em uma política como definindo *como* você quer protegê-la. Se você estiver fazendo backup de todos os bancos de dados ou fazendo backup de todos os sistemas de arquivos de um host, por exemplo, você pode criar um grupo de recursos que inclua todos os bancos de dados ou todos os

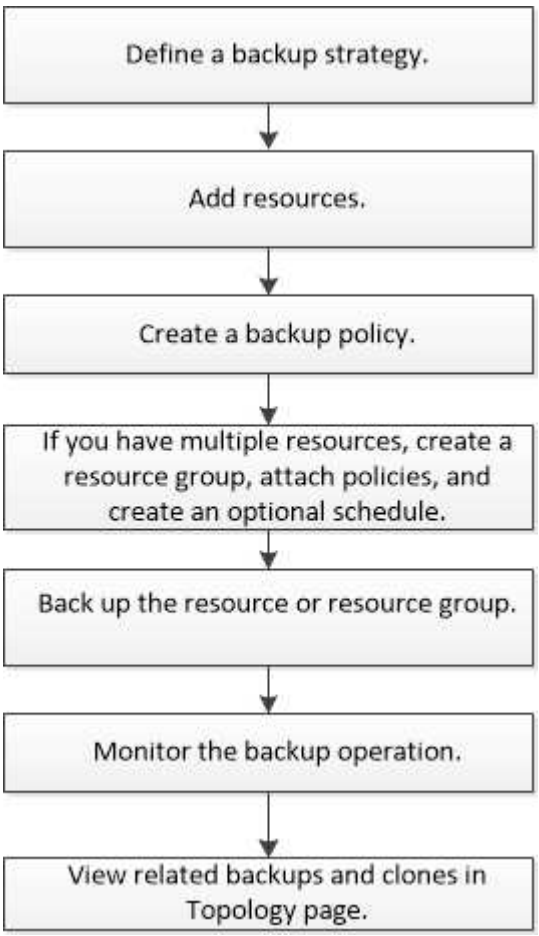
sistemas de arquivos no host. Em seguida, você pode anexar duas políticas ao grupo de recursos: Uma política diária e uma política por hora. Ao criar o grupo de recursos e anexar as políticas, você pode configurar o grupo de recursos para executar um backup baseado em arquivo diariamente e outro agendamento que executa backup baseado em Snapshot por hora.

Fazer backup de recursos de plug-ins compatíveis com NetApp

Fazer backup de recursos de plug-ins compatíveis com NetApp

O fluxo de trabalho de backup inclui Planejamento, identificação dos recursos para backup, gerenciamento de políticas de backup, criação de grupos de recursos e inclusão 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 clone. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte o. "Guia de referência de cmdlet do software SnapCenter"

Adicione recursos aos plug-ins compatíveis com 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 servidor SnapCenter, adicionar hosts, criar conexões do sistema de storage e adicionar credenciais.
- Você deve ter carregado os plug-ins para o servidor SnapCenter.

Passos

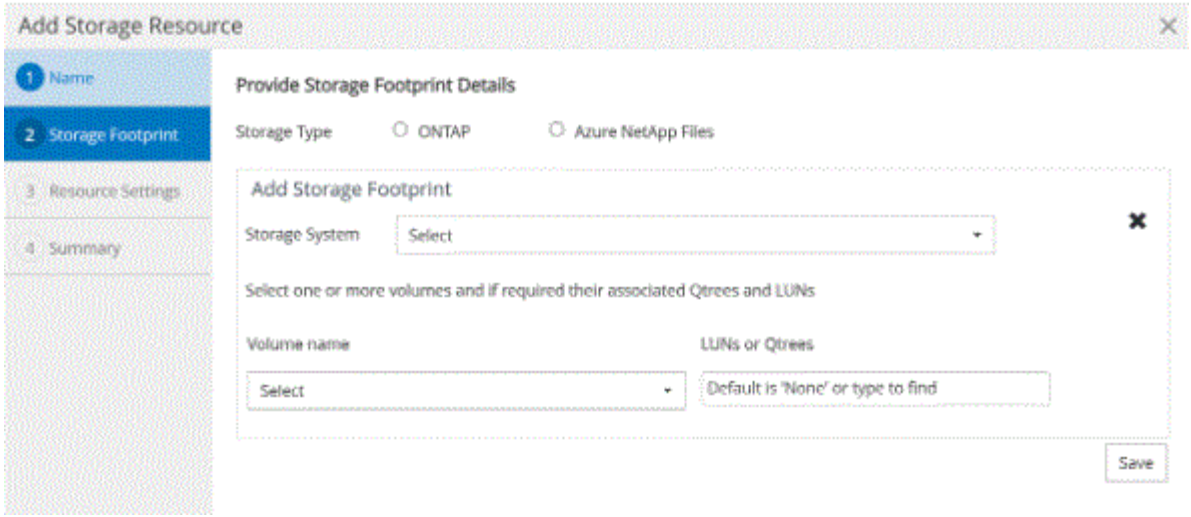
1. No painel de navegação esquerdo, selecione **Resources** e, em seguida, selecione o plug-in apropriado na lista.
2. Na página recursos, selecione **Adicionar recurso**.
3. Na página fornecer detalhes do recurso, execute as seguintes ações:

Para este campo…	Faça isso…
Nome	Introduza o nome do recurso.
Nome do host	Selecione o host.
Tipo	Selecione o tipo. Tipo é definido pelo usuário de acordo com 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.
Monte caminhos	Introduza os caminhos de montagem onde o recurso está montado. Isso é aplicável apenas para um host Windows.

4. Na página fornecer espaço físico de armazenamento, selecione um sistema de armazenamento e escolha um ou mais volumes, LUNs e qtrees e, em seguida, selecione **Salvar**.

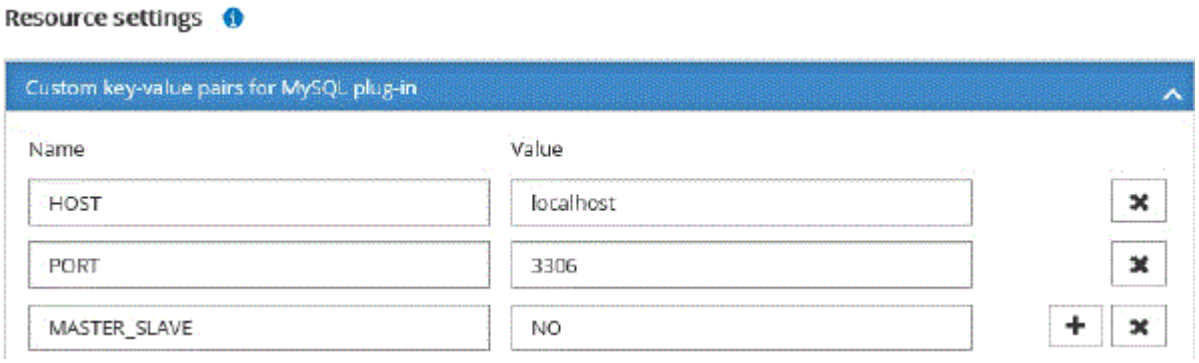
   Opcional: Selecione o ícone para adicionar mais volumes, LUNs e qtrees de outros sistemas de armazenamento.

   Os plug-ins compatíveis com NetApp não oferecem suporte à descoberta automática dos recursos. Os detalhes de armazenamento de ambientes físicos e virtuais também não são descobertos automaticamente. Você precisa fornecer as informações de storage para ambientes físicos e virtuais ao criar os recursos.



5. Na página Configurações de recursos, forneça pares de valor de chave personalizados para o recurso.

   Certifique-se de que o nome das chaves personalizadas está em maiúsculas.



   Para os respetivos parâmetros de plug-in, consulte "Parâmetros para configurar o recurso"

6. Revise o resumo e selecione **Finish**.

Resultado

Os recursos são exibidos juntamente com informações como tipo, nome do host ou cluster, grupos e políticas de recursos associados e status geral.

Você deve atualizar os recursos se os bancos de dados forem renomeados fora do SnapCenter.

Depois de terminar

Se você quiser fornecer acesso aos ativos a outros usuários, o administrador do SnapCenter deve atribuir ativos a esses usuários. Isso permite que os usuários executem as ações para as quais eles têm permissões nos ativos que são atribuídos a eles.

Depois de adicionar os recursos, você pode modificar os detalhes do recurso. Se um recurso de plug-ins compatível com 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 você estiver adicionando os plug-ins manualmente, poderá usar os seguintes parâmetros para configurar o recurso na página Configurações de recursos.

Plug-in para MongoDB

Definições de recursos:

- MONGODB_APP_SERVER(para tipo de recurso como cluster sharded) ou MONGODB_REPLICASE_SERVER(para tipo de recurso como replicaset)
- OPLOG_PATH (parâmetro opcional no caso de ser fornecido a partir de MongoDB.propertiesfile)
- MONGODB_AUTHENTICATION_TYPE (SIMPLES para autenticação LDAP e nenhum para outros)

Você deve fornecer os seguintes parâmetros precisam ser fornecidos n arquivo MongoDB.properties:

- DISABLE_STARTING_STARTING_SERVICES
  - N se os serviços de arranque/paragem forem executados pelo plug-in.
  - Y se iniciar/**parar serviços são executados pelo usuário.
  - Parâmetro opcional como valor padrão é definido como N.
- OPLOG_PATH_ (parâmetro opcional no caso de já ser fornecido como par chave-valor personalizado no SnapCenter).

Plug-in para MaxDB

Definições de recursos:

- XUSER_ENABLE (Y|N) ativa ou desativa o uso de um xuser para MaxDB para que uma senha não seja necessária para o usuário do banco de dados.
- HANDLE_LOGWRITER (Y|N) executa as operações de suspender o gravador de log (N) ou retomar logwriter (Y).
- DBMCLICMD (path_to_dbmcli_cmd) especifica o caminho para o comando MaxDB dbmcli. Se não estiver definido, dbmcli no caminho de pesquisa será usado.

  Para o ambiente Windows, o caminho deve estar entre aspas duplas ("…").

- SQLCLICMD (path_to_sqlcli_cmd) especifica o caminho para o comando sqlcli MaxDB. Se o caminho não estiver definido, sqlcli é usado no caminho de pesquisa.
- MAXDB_UPDATE_HIST_LOG (Y|N) instrui o programa de backup MaxDB 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 Snapshot do Snap Creator é bem-sucedida e garante que o snapshot seja criado.

  Isso se aplica somente a 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 tem de existir e ser um tipo externo de modelo de cópia de segurança. Para habilitar a integração de snapshot para o MaxDB 7,8 e posterior, você deve ter a funcionalidade de servidor em segundo plano do MaxDB e modelo de backup do MaxDB já configurado do tipo EXTERNO.

- 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 deve 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

Definições de recursos:

- SYBASE_SERVER (data_Server_NAME) especifica o nome do servidor de dados Sybase (-S opção 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.

  Necessário para UNIX. Esse parâmetro é necessário se o usuário executando os comandos de início e parada do Snap Creator Agent (geralmente o usuário raiz) e o usuário executando o comando isql forem diferentes.

- SYBASE_TRAN_DUMP dB_name:Directory_path permite que você execute um despejo de transação Sybase depois de 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 (Y|N) ativa ou desativa a compressão de despejo de transação Sybase nativa.
- SYBASE_ISQL_CMD (por exemplo, /opt/sybase/OCS-15_0/bin/isql) define o caminho para o comando isql.
- SYBASE_EXCLUDE_TEMPDB (Y|N) permite excluir automaticamente bancos de dados temporários criados pelo usuário.

Plug-in para aplicativos Oracle (ORASCPM)

Definições 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 o 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 você deve fazer o backup dos logs do arquivo ou não.
- ORACLE_BACKUPMODE especifica se o backup deve ser realizado 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>*. Isso normalmente ocorre 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 compatíveis com o NetApp

Antes de usar o SnapCenter para fazer backup de recursos específicos de plug-in compatíveis com o NetApp, você deve criar uma política de backup para o recurso ou grupo de recursos que 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 deve ter se preparado para a proteção de dados.

  A preparação para a proteção de dados inclui tarefas como a instalação do SnapCenter, a adição de hosts, a criação de conexões do sistema de storage e a adição de 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 os SVMs para os volumes de origem e destino a você se estiver replicando snapshots em um espelho ou cofre.

- Você deve ter adicionado manualmente os recursos que deseja proteger.

Sobre esta tarefa

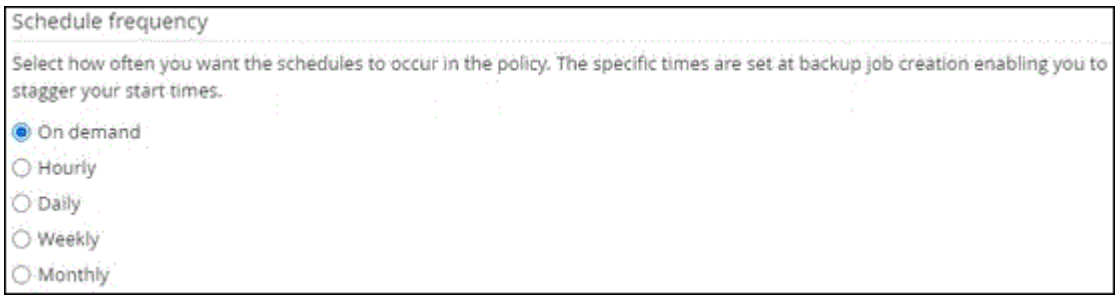
- Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e retém backups. Além disso, você pode especificar as configurações de replicação, script e aplicativo.
- Especificar opções em uma política economiza tempo quando você deseja reutilizar a política para outro grupo de recursos.
- SnapLock
  - Se a opção 'reter as cópias de backup para um número específico de dias' estiver selecionada, o período de retenção do SnapLock deve ser menor ou igual aos dias de retenção mencionados.
  - Especificar um período de bloqueio instantâneo impede a exclusão dos instantâneos até que o período de retenção expire. Isso pode levar a reter um número maior de instantâneos do que a contagem especificada na política.
  - Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

As configurações do SnapLock primário são gerenciadas na política de backup do SnapCenter e as configurações do SnapLock secundário 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 a descrição da política.
5. Na página Configurações, execute as seguintes etapas:
   - Especifique o tipo de agendamento selecionando **on demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.

     Você pode especificar a programação (data de início, data de término e frequência) para a operação de backup enquanto cria 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 diferentes programações de backup a cada política.

     Se você tiver agendado para as 2:00 da manhã, o horário não será acionado durante o horário de verão (DST).

   - Na seção Configurações personalizadas de backup, forneça quaisquer configurações específicas de backup que tenham que ser passadas para o formato de valor de chave do plug-in. Você pode fornecer vários valores-chave a serem passados para o plug-in.
6. Na página **retenção**, 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 instantâneos	Selecione **Total de cópias Snapshot a manter** e especifique o número de capturas instantâneas que deseja manter. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro. Você deve definir a contagem de retenção como 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino. O valor máximo de retenção é 1018 para recursos no ONTAP 9.4 ou posterior e 254 para recursos no ONTAP 9.3 ou anterior. Os backups falharão se a retenção for definida para um valor maior do que o que a versão subjacente do ONTAP suporta.
Mantenha as capturas instantâneas por um determinado número de dias	Selecione **manter cópias Snapshot para** e especifique o número de dias para os quais deseja manter as capturas instantâneas antes de excluí-las.
Período de bloqueio de cópias snapshot	Selecione período de bloqueio instantâneo e selecione dias, meses ou anos. O período de retenção do SnapLock deve ser inferior a 100 anos.

7. Na página **replicação**, especifique as configurações de replicação:

Para este campo…	Faça isso…
Atualizar SnapMirror depois de criar uma cópia Snapshot local	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Se a relação de proteção no ONTAP for do tipo espelho e Cofre e se você selecionar somente essa opção, instantâneo criado no primário não será transferido para o destino, mas será listado no destino. Se este instantâneo for selecionado no destino para executar uma operação de restauração, a seguinte mensagem de erro será exibida: Local secundário não está disponível para o backup abobadado/espelhado 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. "Veja os backups e clones relacionados a recursos de plug-in compatíveis com o NetApp na página topologia"Consulte .
Atualizar SnapVault depois de criar uma cópia Snapshot local	Selecione esta opção para executar a replicação de backup disco a disco (backups 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 apenas no secundário do ONTAP conhecido como SnapLock Vault, clicar no botão **Atualizar** na página topologia atualiza o período de bloqueio no secundário que é recuperado do ONTAP. Para obter mais informações sobre o SnapLock Vault, consulte confirmar snapshots para WORM em um destino de cofre "Veja os backups e clones relacionados a recursos de plug-in compatíveis com o NetApp na página topologia".

Para este campo…	Faça isso…
Etiqueta de política secundária	Selecione uma etiqueta Snapshot. Dependendo do rótulo de captura instantânea selecionado, o ONTAP aplica a política de retenção de snapshot secundária que corresponde ao rótulo. Se você selecionou **Atualizar SnapMirror depois de criar uma cópia Snapshot local**, você pode especificar opcionalmente o rótulo de política secundária. No entanto, se você selecionou **Atualizar SnapVault depois de criar uma cópia Snapshot local**, especifique o rótulo de política secundária.
Contagem de tentativas de erro	Introduza o número máximo de tentativas de replicação que podem ser permitidas antes de a operação parar.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o storage secundário para evitar atingir o limite máximo de snapshots no storage secundário.

8. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas

Um grupo de recursos é o contentor ao qual você deve adicionar recursos que deseja fazer backup e proteger. Ele permite fazer backup de todos os dados associados a uma determinada aplicação simultaneamente. Você também deve anexar uma ou mais políticas ao grupo de recursos para definir o tipo de tarefa de proteção de dados que deseja executar.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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	Introduza um nome para o grupo de recursos. Observação: O nome do grupo de recursos não deve exceder 250 carateres.

Para este campo…	Faça isso…
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos. Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.
Use o formato de nome personalizado para cópia Snapshot	Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea. Por exemplo, *customtext_resource group_policy_hostname ou resource group_hostname*. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

4. Opcional: Na página recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Resource Type**.

   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 da aplicação**, faça o seguinte:

   a. Selecione a seta backups para definir opções adicionais de backup:

      Ative o backup do grupo de consistência e execute as seguintes tarefas:

Para este campo…	Faça isso…
Tenha tempo para esperar que a operação de snapshot do grupo de consistência seja concluída	Selecione urgente, Médio ou relaxado para especificar o tempo de espera para que a operação Snapshot seja concluída. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a 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 quiesce, Snapshot e unquiesce. Também pode introduzir os pré comandos a serem executados antes de sair em caso de falha.

b. Selecione a seta Configurações personalizadas e insira os pares de valor de chave personalizados necessários para todas as operações de proteção de dados usando esse recurso.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_ENABLE	(Y/N)	Permite que a gestão do registo de arquivo elimine os registos de arquivo.
ARCHIVE_LOG_RETENÇÃO	number_of_days	Especifica o número de dias em que os logs de arquivo são mantidos. Esta definição tem de ser igual ou superior a NTAP_SNAPSHOT_ RETENÇÕES.
ARCHIVE_LOG_DIR	change_info_directory/logs	Especifica o caminho para o diretório que contém os logs do arquivo.

Parâmetro	Definição	Descrição
ARCHIVE_LOG_EXT	extensão_ficheiro	Especifica o comprimento da extensão do arquivo de log do arquivo. Por exemplo, se o log de arquivo for log_backup_0_0_0_0,161518551942 9 e se o valor file_extension for 5, a extensão do log manterá 5 dígitos, que é 16151.
ARCH ARCHIVE_LOG_RECURSIVE_SE	(Y/N)	Permite o gerenciamento de logs de arquivo dentro de subdiretórios. Você deve usar este parâmetro se os logs do arquivo estiverem localizados em subdiretórios.

c. Selecione a seta **Snapshot Copy Tool** 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 instantâneo. Para recursos do Linux, essa opção não é aplicável.	Selecione **SnapCenter com consistência do sistema de arquivos**. Esta opção não é aplicável ao plug-in SnapCenter para banco de dados SAP HANA.
SnapCenter para criar um instantâneo no nível de storage	Selecione **SnapCenter sem consistência do sistema de arquivos**.
Para inserir o comando a ser executado no host para criar Snapshots.	Selecione **Other** e digite o comando a ser executado no host para criar uma captura Instantânea.

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 são listadas na seção **Configurar programações para políticas selecionadas**.

b. Na coluna **Configurar agendas**, selecione para a política que deseja configurar.

c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e

selecione OK.

Onde policy_name é o nome da política selecionada.

As programações configuradas são listadas na coluna agendas aplicadas. As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas de backup do SnapCenter.

8. Na lista suspensa **preferência de e-mail** na página **notificação**, 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 servidor SMTP deve ser configurado em **Configurações** > **Configurações globais**.

9. Revise o resumo e selecione **Finish**.

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 Administrador da infraestrutura para criar conexões de armazenamento.
- Você deve garantir que as instalações do plug-in não estão em andamento.

  As instalações de plug-in do host não devem estar em andamento ao adicionar uma conexão de sistema de armazenamento, pois 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 do sistema de armazenamento devem ser exclusivos.

  O SnapCenter não é compatível com vários sistemas de storage com o mesmo nome em clusters diferentes. Cada sistema de storage com suporte do SnapCenter deve ter um nome exclusivo e um endereço IP de 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Fazer backup de recursos de plug-ins compatíveis com NetApp individuais

Se um recurso de plug-ins com suporte do NetApp individual não fizer parte de qualquer grupo de recursos, você poderá fazer o backup do recurso na página recursos. Você pode fazer backup do recurso sob demanda ou, se o recurso tiver uma política anexada e uma programação configurada, os backups ocorrem automaticamente de acordo com a programação.

Antes de começar

- Você deve ter criado uma política de backup.
- Se você quiser fazer backup de um recurso que tenha uma relação SnapMirror com um armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror All'". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Clique em e selecione o nome do host e o tipo de recurso para filtrar os recursos. Em seguida, pode clicar para fechar o painel de filtro.
3. Clique no recurso que você deseja fazer backup.
4. Na página recurso, se você quiser usar um nome personalizado, marque a caixa de seleção **usar formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado para o nome da captura Instantânea.

   Por exemplo, *customtext_policy_hostname* ou *resource_hostname*. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.
5. Na página Configurações do aplicativo, faça o seguinte:

   a. Clique na seta **backups** para definir opções adicionais de backup:

      Ative o backup do grupo de consistência, se necessário, e execute as seguintes tarefas:

Para este campo…	Faça isso…
Tenha tempo para esperar que a operação de snapshot do grupo de consistência seja concluída	Selecione urgente, Médio ou relaxado para especificar o tempo de espera para que a operação Snapshot seja concluída. Urgente: 5 segundos, Médio: 7 segundos e relaxado: 20 segundos.
Desativar a sincronização WAFL	Selecione esta opção para evitar forçar um ponto de consistência WAFL.

   +

a. Clique na seta **Scripts** para executar comandos pré e POST para operações quiesce, Snapshot e unquiesce. Você também pode executar pré-comandos antes de sair da operação de backup.

   Os Prescripts e postscripts são executados no servidor SnapCenter.

b. Clique na seta **Custom Configurations** (Configurações personalizadas) e insira os pares de valores personalizados necessários para todos os trabalhos que usam esse recurso.

c. Clique na seta **Snapshot Copy Tool** para selecionar a ferramenta para criar instantâneos:

Se você quiser…	Então…
SnapCenter para tirar uma Snapshot no nível de storage	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 depois tirar uma Snapshot	Selecione **SnapCenter com consistência do sistema de arquivos**.
Para inserir o comando para criar uma captura Instantânea	Selecione **Other** e, em seguida, digite o comando para criar uma captura Instantânea.

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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique na coluna Configurar agendas para a política para a qual você deseja configurar um

agendamento.

c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e clique em **OK**.

Onde, *policy_name* é o nome da política selecionada.

As programações configuradas são listadas na coluna agendas aplicadas.

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 **Finish**.

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 tiver aplicado 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. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter para um usuário especificado usando o cmdlet Open-SmConnection.

```
Open-smconnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146\
```

É apresentado o aviso de nome de utilizador e palavra-passe.

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. Exiba o status da tarefa de backup usando o cmdlet Get-SmBackupReport.

   Este exemplo exibe um relatório de resumo de todos os trabalhos 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-in compatíveis com o 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 uma programação configurada, os backups ocorrerão automaticamente de acordo com a programação.

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 uma relação SnapMirror com o armazenamento secundário, a função ONTAP atribuída ao usuário de armazenamento deve incluir o privilégio "'SnapMirror

All'". No entanto, se você estiver usando a função "vsadmin", o privilégio "SnapMirror all" não será necessário.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 e selecionando a tag. Em seguida, pode clicar para fechar o painel de filtro.
3. Na página grupos de recursos, selecione o grupo de recursos que deseja fazer backup e clique em **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. Clique em **Backup**.
5. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.
   - Nas configurações do MetroCluster, o SnapCenter pode não ser capaz de detetar uma relação de proteção após um failover.

     "Não é possível detetar a relação SnapMirror ou SnapVault após o failover do MetroCluster"
   - Se você estiver fazendo backup de dados de aplicativos em VMDKs e o tamanho de heap Java para o plug-in SnapCenter para VMware vSphere não for grande o suficiente, o backup pode falhar. Para aumentar o tamanho do heap Java, localize o arquivo de script /opt/NetApp/init_scripts/scvservice. Nesse script, o `do_start method` comando inicia o serviço de plug-in SnapCenter VMware. Atualize esse comando para o seguinte: `Java -jar -Xmx8192M -Xms4096M`.

Monitorar as operações de backup de recursos de plug-in compatíveis com NetApp

Você pode monitorar o progresso de diferentes operações de backup usando a página SnapCenterJobs. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado correspondente das operações:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos

- Em fila de espera
- 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 a que apenas as operações de cópia de segurança sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Backup**.
   d. Na lista suspensa **Status**, selecione o status da cópia de segurança.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.

   Embora o status do trabalho de backup seja exibido , quando você clica nos detalhes do trabalho, você pode ver que algumas das tarefas secundárias da operação de backup ainda estão em andamento ou marcadas com sinais de aviso.

5. Na página Detalhes da tarefa, clique em **Exibir logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Cancelar operações de backup para plug-ins compatíveis com NetApp

Você pode cancelar as operações de backup que estão na fila.

O que você vai precisar

- Você deve estar logado como administrador do SnapCenter ou proprietário do trabalho para cancelar as operações.
- Você pode cancelar uma operação de backup na página **Monitor** ou no painel **atividade**.
- Não é possível cancelar uma operação de cópia de segurança em execução.
- Você pode usar os comandos GUI, cmdlets do SnapCenter ou CLI para cancelar as operações de backup.
- O botão **Cancelar trabalho** está desativado 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 em fila de outros membros enquanto usa essa função.

Passos

1. Execute uma das seguintes ações:

A partir 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 da atividade	a. Depois de iniciar a operação de backup, clique em no painel atividade para exibir as cinco operações mais recentes. b. Selecione a operação. c. Na página Detalhes da tarefa, clique em **Cancelar tarefa**.

A operação é cancelada e o recurso é revertido para o estado anterior.

Veja os backups e clones relacionados a recursos de plug-ins compatíveis com o NetApp na página topologia

Ao se preparar para fazer backup ou clonar um recurso, talvez seja útil exibir uma representação gráfica de todos os backups e clones no storage primário e secundário. Na página topologia, você pode ver todos os backups e clones disponíveis para o grupo de recursos ou recursos selecionado. Você pode visualizar os detalhes desses backups e clones e, em seguida, selecioná-los para executar operações de proteção de dados.

Sobre esta tarefa

Você pode revisar os ícones a seguir na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no storage primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups e clones disponíveis no storage primário.
- Exibe o número de backups e clones espelhados no storage secundário usando a tecnologia SnapMirror.

  Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

- Exibe o número de backups e clones replicados no storage secundário usando a tecnologia SnapVault.

  O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou backups 6 usando uma política para reter apenas 4 backups, o número de backups exibidos será 6.

Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o recurso ou o 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 de resumo para ver um resumo do número de backups e clones disponíveis no storage 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, clique no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Um horário semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o recurso do aplicativo é espalhado por vários volumes, o tempo de expiração do SnapLock para o backup será o tempo de expiração do SnapLock mais longo definido para um snapshot em um volume. O tempo de expiração mais longo do SnapLock é recuperado do ONTAP.

   Após o backup sob demanda, clicando no botão **Refresh** atualiza os detalhes do backup ou clone.

5. No modo de 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 um 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 estão 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 para excluir o clone.

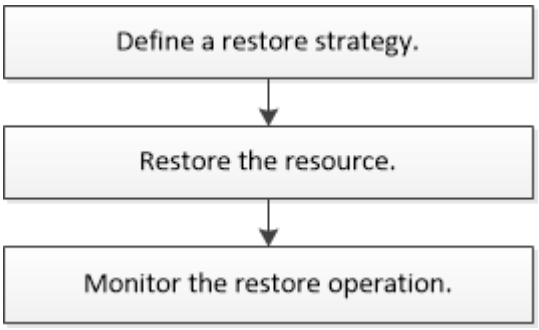
Restaure os recursos de plug-ins compatíveis com o NetApp

Restaure os recursos de plug-in compatíveis com o NetApp

O fluxo de trabalho de restauração e recuperação inclui Planejamento, execução das 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 clone. Para obter informações sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte "Guia de referência de cmdlet do software SnapCenter" .

Restaurar um backup de recursos

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 dos grupos de recursos ou recursos.
- O administrador do SnapCenter deve ter atribuído a você as máquinas virtuais de storage (SVMs) para os volumes de origem e de destino se você estiver replicando snapshots em um espelho ou cofre.
- Você deve ter cancelado qualquer operação de backup que esteja atualmente em andamento para o grupo de recursos ou recursos que deseja restaurar.

Sobre esta tarefa

- A operação de restauração padrão somente restaura objetos de armazenamento. As operações de restauração no nível da aplicação só podem ser executadas se o plug-in suportado pela NetApp fornecer essa capacidade.
- Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com informações como tipo, nome do host ou cluster, grupos e políticas de recursos associados e status.

   Embora um backup possa ser para um grupo de recursos, ao restaurar, você deve selecionar os recursos individuais que deseja restaurar.

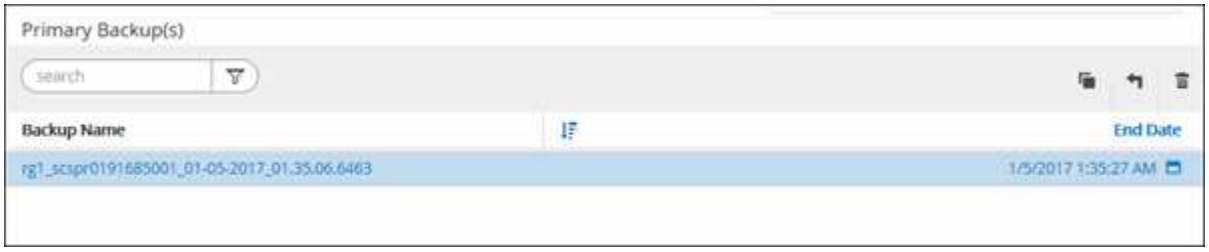
   Se o recurso não estiver protegido, *não protegido* será exibido na coluna **Estado geral**.

   O status *não protegido* na coluna **Estado geral** pode significar que o recurso não está protegido ou que o recurso foi protegido 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 do recurso é exibida.

4. Na exibição **Gerenciar cópias**, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Na tabela backup(s) primário(s), selecione o backup do qual você deseja restaurar e clique em .



6. Na página Restaurar escopo, selecione **recurso completo** ou **nível de arquivo**.
   a. Se você selecionou **Complete Resource**, 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 **File Level**, então você pode selecionar **All** ou selecionar volumes ou qtrees e, em seguida, inserir o caminho relacionado aos volumes ou qtrees que são selecionados separados por vírgulas.
      - Você pode selecionar vários volumes e qtrees.
      - Se o tipo de recurso for LUN, todo o LUN será restaurado. Pode selecionar vários LUNs. Observação: Se você selecionar **All**, todos os arquivos nos volumes, qtrees ou LUNs serão restaurados.
7. Na página **Pré-operações**, insira pré-restaurar e desmontar comandos para serem executados antes

de executar um trabalho de restauração.

8. Na página **Post OPS**, insira os comandos mount e POST Restore para serem executados após a execução de 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 **Finish**.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 29th 2015 de janeiro a 3rd 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 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Monitorar as operações de restauração de recursos de plug-in compatíveis com o NetApp

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um 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 executar.

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Restore**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Clone NetApp compatível com backups de recursos de plug-ins

Clone NetApp compatível com backups de recursos de plug-ins

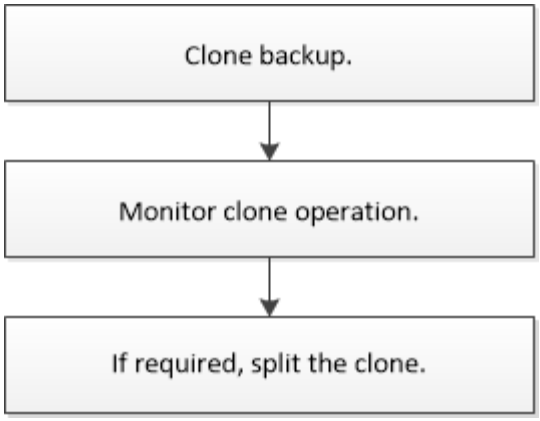
O fluxo de trabalho do clone inclui a execução da operação de clone e o monitoramento da operação.

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 de aplicativos
- 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 clone:



Você também pode usar cmdlets do PowerShell manualmente ou em scripts para executar operações de backup, restauração e clone. Para obter informações detalhadas sobre cmdlets do PowerShell, use a ajuda do cmdlet SnapCenter ou consulte "Guia de referência de cmdlet do software SnapCenter" .

Clone de um backup

Você pode usar o SnapCenter para clonar um backup. Você pode clonar do backup primário ou secundário. As funcionalidades das operações de clone 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 clone padrão somente clona objetos de storage. As operações de clone no nível da aplicação só podem ser executadas se o plug-in compatível com NetApp fornecer essa funcionalidade.
- Você deve garantir que os agregados que hospedam os volumes estejam na lista de agregados atribuídos da máquina virtual de storage (SVM).

Sobre esta tarefa

Para a versão ONTAP 9.12,1 e inferior, os clones criados a partir dos instantâneos do Vault do SnapLock como parte da restauração herdarão o tempo de expiração do SnapLock Vault. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.

IU do SnapCenter

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página **recursos**, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.

   Os recursos são exibidos juntamente com informações como tipo, nome do host ou cluster, grupos e políticas de recursos associados e status.

3. Selecione o grupo de recursos ou recursos.

   Você deve selecionar um recurso se selecionar um grupo de recursos.

   A página de topologia do grupo de recursos ou recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Selecione o backup de dados na tabela e clique em .
6. Na página locais, execute 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 está instalado.
Sufixo clone	Isso é obrigatório quando o destino do clone é o mesmo que a origem. Digite 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 que o recurso original, forneça um sufixo para diferenciar o recurso clonado do recurso original; caso contrário, a operação falha.

   Se o recurso selecionado for um LUN e se você estiver clonando de um backup secundário, os volumes de destino serão listados. Uma única fonte pode ter vários volumes de destino.

7. Na página **Configurações**, execute o seguinte:

Para este campo…	Faça isso…
Nome do iniciador	Insira o nome do iniciador do host, que é IQDN ou WWPN.

Para este campo…	Faça isso…
Protocolo Igroup	Selecione Igroup Protocol (Protocolo de grupo).

A página de definições é apresentada apenas se o tipo de armazenamento for LUN.

8. Na página Scripts, insira os comandos para pré-clone ou pós-clone que devem ser executados antes ou depois da operação clone, respetivamente. Digite o comando mount para montar um sistema de arquivos em um host.

   Por exemplo:

   - Comando pre clone: Exclua bancos de dados existentes com o mesmo nome
   - Comando Post clone: Verifique um banco de dados ou inicie um banco de dados.

     Montar comando 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 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.

10. Revise o resumo e clique em **Finish**.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Cmdlets do PowerShell

Passos

1. Inicie uma sessão de conexão com o servidor SnapCenter 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 clone a partir de um grupo de recursos de clone ou de um backup existente usando o cmdlet New-SmClone.

   Este exemplo cria um clone a partir 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. Exiba o status da tarefa clone usando o cmdlet Get-SmCloneReport.

   Este exemplo exibe um relatório de clone para a ID de tarefa especificada:

```
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 as operações de clone de recurso de plug-in compatíveis com o NetApp

Você pode monitorar o andamento das operações de clone do SnapCenter usando a página tarefas. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.

3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista para que apenas operações de clone sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Proteja 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 é instalado em seu ambiente, você pode 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
- Faça backup de sistemas de arquivos Unix
- Agendar operações de backup
- Restaure backups do sistema de arquivos
- Clonar backups do sistema de arquivos
- Monitore operações de backup, restauração e clone

Configurações compatíveis

Item	Configuração suportada
Ambientes	• Servidor físico • Servidor virtual Armazenamentos de dados da Vevolve em NFS e SAN. O armazenamento de dados da Vevolve só pode ser provisionado com as ferramentas do ONTAP para VMware vSphere.
Sistemas operacionais	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
Sistemas de arquivos	• SAN: ◦ Sistemas de arquivos baseados em LVM e não em LVM ◦ LVM sobre VMDK ext3, ext4 e xfs • NFS: NFS v3, NFS v4.x
Protocolos	• FC • FCoE • ISCSI • NFS

Item	Configuração suportada
Multipath	sim

Limitações

- A combinação de RDMs e discos virtuais em um grupo de volumes não é suportada.
- A restauração no nível do arquivo não é suportada.

  No entanto, você pode executar manualmente a restauração no nível do arquivo clonando o backup e copiando os arquivos manualmente.

- A combinação de sistemas de arquivos espalhados por VMDKs provenientes do armazenamento de dados NFS e VMFS não é compatível.
- NVMe não é compatível.
- O provisionamento não é compatível.

Instale o plug-in SnapCenter para sistemas de arquivos Unix

Pré-requisitos para adicionar hosts e instalar o pacote Plug-ins para Linux

Antes de adicionar um host e instalar o pacote de plug-ins para Linux, você deve completar todos os requisitos.

- Se estiver a utilizar iSCSI, o serviço iSCSI tem de estar em execução.
- Você pode usar a autenticação baseada em senha para o usuário root ou não root ou autenticação baseada em chave SSH.

  O plug-in do SnapCenter para sistemas de arquivos Unix pode ser instalado por um usuário não-root. No entanto, você deve configurar o sudo Privileges para que o usuário não-root instale e inicie o processo de plug-in. Depois de instalar o plug-in, os processos serão executados como um usuário não-root eficaz.

- Crie credenciais com o modo de autenticação como Linux para o usuário de instalação.
- Você deve ter instalado o Java 11 em seu host Linux.

  Certifique-se de ter instalado apenas a edição certificada DO Java 11 no host Linux.

  Para obter informações sobre O download DO JAVA, consulte: "Downloads Java para todos os sistemas operacionais"

- Você deve ter **bash** como o shell padrão para instalação do plug-in.

Requisitos de 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 • SUSE Linux Enterprise Server (SLES)
RAM mínima para o plug-in SnapCenter no host	2 GB
Espaço mínimo de instalação e log para o plug-in SnapCenter no host	2 GB Deve alocar espaço em disco suficiente e monitorizar o consumo de armazenamento pela pasta de registos. O espaço de registo necessário varia consoante o número de entidades a proteger e a frequência das operações de proteçãoão 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 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, você deve garantir que a opção JAVA_HOME localizada em /var/opt/SnapCenter/spl/etc/spl.properties esteja definida para a versão JAVA correta e o caminho correto.

Para obter as informações mais recentes sobre versões suportadas, consulte o "Ferramenta de Matriz de interoperabilidade do NetApp".

Adicione hosts e instale o pacote Plug-ins para Linux usando 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 guia **hosts gerenciados** está selecionada na parte superior.

3. Clique em **Add**.
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	Insira o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host. O SnapCenter depende da configuração adequada do DNS. Portanto, a melhor prática é entrar no FQDN. Se você estiver adicionando um host usando o SnapCenter e o host 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 as informações sobre como criar credenciais. Você pode exibir 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	Guarde o número da porta padrão ou especifique o número da porta. O número da porta padrão é 8145. Se o servidor SnapCenter tiver sido 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, você deve especificar a mesma porta. Caso contrário, a operação falha.
Caminho de instalação	O caminho padrão é */opt/NetApp/SnapCenter*. Opcionalmente, você pode personalizar o caminho. Se você usar o caminho personalizado, verifique se o conteúdo padrão dos sudoers é atualizado com o caminho personalizado.
Ignorar verificações de pré-instalação opcionais	Marque essa 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 selecionado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar 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 for especificado nas regras de rejeição do firewall.

   Mensagens de erro ou aviso apropriadas são 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: SnapCenter NetApp para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deve corrigir o problema.

   Em uma configuração de HA, se você estiver atualizando o arquivo web.config, será necessário atualizar o arquivo em ambos os nós.

8. Verifique a impressão digital e clique em **Confirm and Submit**.

   O SnapCenter não suporta o algoritmo ECDSA.

   A verificação de impressões digitais é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

9. Monitorize 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 automaticamente descobertos e exibidos na Página de recursos. Se nada for exibido, clique em **Atualizar recursos**.

Monitorar o status da instalação

Pode monitorizar o progresso da instalação do pacote de plug-ins do SnapCenter utilizando a página trabalhos. Você pode querer verificar o andamento da instalação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, para filtrar a lista de modo a que apenas as operações de instalação de plug-in sejam listadas, faça o seguinte:
   a. Clique em **filtro**.
   b. Opcional: Especifique a data de início e fim.
   c. No menu suspenso tipo, selecione **Instalação 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 **Visualizar logs**.

Configure o serviço SnapCenter Plug-in Loader

O serviço SnapCenter Plug-in Loader carrega o pacote plug-in para que o Linux interaja com o servidor SnapCenter. O serviço SnapCenter Plug-in Loader é instalado quando você instala o pacote de plug-ins do SnapCenter para Linux.

Sobre esta tarefa

Depois de instalar o pacote de plug-ins do SnapCenter para Linux, o serviço Loader do plug-in do SnapCenter é iniciado automaticamente. Se o serviço Loader de plug-in do SnapCenter não for iniciado automaticamente, você deve:

- Certifique-se de que o diretório em que o plug-in está a funcionar não é eliminado
- Aumente o espaço de memória atribuído à Máquina Virtual Java

O arquivo spl.properties, que está localizado em */custom_location/NetApp/SnapCenter/spl/etc/*, contém os seguintes parâmetros. Os valores padrão são atribuídos a esses parâmetros.

Nome do parâmetro	Descrição
LOG_LEVEL	Apresenta os níveis de registo suportados. Os valores possíveis são TRACE, DEBUG, INFO, WARN, ERROR e FATAL.
SPL_PROTOCOL (PROTOCOLO SPL)	Apresenta o protocolo suportado pelo Plug-in Loader SnapCenter. Apenas o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver ausente.
SnapCenter_SERVER_PROTOCOL	Apresenta o protocolo suportado pelo servidor SnapCenter. Apenas o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver ausente.
SKIP_JAVAHOME_UPDATE	Por padrão, o serviço SPL deteta o caminho java e atualiza o parâmetro Java_HOME. Portanto, o valor padrão é definido como FALSE. Você pode definir como VERDADEIRO se quiser desativar o comportamento padrão e corrigir manualmente o caminho java.
SPL_KEYSTORE_PASS	Exibe a senha do arquivo keystore. Você pode alterar esse valor somente se você alterar a senha ou criar um novo arquivo de keystore.
SPL_PORT	Exibe o número da porta na qual o serviço Plug-in Loader do SnapCenter está sendo executado. Você pode adicionar o valor se o valor padrão estiver ausente. Você não deve alterar o valor depois de instalar os plug-ins.

Nome do parâmetro	Descrição
SnapCenter_Server_HOST	Exibe o endereço IP ou o nome do host do servidor SnapCenter.
SPL_KEYSTORE_PATH	Exibe o caminho absoluto do arquivo keystore.
SnapCenter_SERVER_PORT	Exibe o número da porta na qual o servidor SnapCenter está sendo executado.
REGISTOS_MAX_COUNT	Exibe o número de arquivos de log do Loader do plug-in do SnapCenter que são retidos na pasta */custom_location/SnapCenter/spl/logs*. O valor padrão é definido como 5000. Se a contagem for superior ao 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 Loader Plug-in SnapCenter 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 da inicialização do SPL.
LOG_MAX_SIZE	Apresenta o tamanho máximo do ficheiro de registo de trabalhos. Assim que o tamanho máximo for atingido, o ficheiro de registo é zipado e os registos são gravados no novo ficheiro desse trabalho.
RETER_LOGS_OF_LAST_DAYS	Exibe o número de dias até os quais os logs são mantidos.
ENABLE_CERTIFICATE_VALIDATION	Exibe verdadeiro quando a validação do certificado CA está ativada para o host. Você pode ativar ou desativar esse parâmetro editando o spl.properties ou usando a GUI ou cmdlet do SnapCenter.

Se algum destes parâmetros não estiver atribuído ao valor predefinido ou se pretender atribuir ou alterar o

valor, pode modificar o ficheiro spl.properties. Você também pode verificar o arquivo spl.properties e editar o arquivo 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 um 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 um usuário não-root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

       Você pode usar a opção -force com o comando stop para parar o serviço SnapCenter Plug-in Loader com força. No entanto, você deve ter cuidado antes de fazê-lo, porque ele também termina as operações existentes.
   - Reinicie o serviço SnapCenter Plug-in Loader:
     - Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - Como um 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 um 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 um usuário não-root, execute: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Configure o 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 armazenamento de confiança SPL e configurar o par de chaves assinadas CA para o armazenamento de confiança 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', tanto como seu armazenamento de confiança e armazenamento de chaves.

Gerenciar senha para o armazenamento de chaves SPL e alias do par de chaves assinadas CA em uso

Passos

1. Você pode recuperar a senha padrão do keystore SPL do arquivo de propriedade SPL.

   É o valor correspondente à chave 'SPL_KEYSTORE_PASS'.

2. Altere a senha do keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Altere a senha para 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 depois de alterar a senha.

A senha para o keystore SPL e para todos os alias associados da chave privada deve ser a mesma.

Configure certificados raiz ou intermediários para o armazenamento de confiança SPL

Você deve configurar os certificados raiz ou intermediários sem a chave privada para o armazenamento de confiança SPL.

Passos

1. Navegue até a pasta que contém o keystore SPL: */var/opt/SnapCenter/spl/etc*.
2. Localize o arquivo 'keystore.jks'.
3. Liste 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 depois de configurar os certificados raiz ou
intermédios para o armazenamento de confiança SPL.
```

Você deve adicionar o certificado de CA raiz e, em seguida, os certificados de CA intermediários.

Configure o par de chaves assinadas da CA para o armazenamento de confiança SPL

Você deve configurar o par de chaves assinadas da CA para o armazenamento de confiança SPL.

Passos

1. Navegue até a pasta que contém o keystore /var/opt/SnapCenter/spl/etc. do SPL
2. Localize o arquivo 'keystore.jks'.
3. Liste 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
. Liste os certificados adicionados no keystore.
```

```
 keytool -list -v -keystore keystore.jks
. Verifique se o keystore contém o alias correspondente ao novo
certificado da CA, que foi adicionado ao keystore.
. Altere a senha da chave privada adicionada para o certificado da 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 espaço ou
carateres especiais ("*",","), altere o nome do alias para um nome
simples:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configure o nome do alias a partir do keystore localizado no arquivo
spl.properties.
```

Atualize este valor com a chave SPL_CERTIFICATE_ALIAS.

4. Reinicie o serviço depois de configurar o par de chaves assinadas pela CA para o armazenamento de confiança SPL.

Configurar a lista de revogação de certificados (CRL) para SPL

Você deve configurar a CRL para SPL

Sobre esta tarefa

- O SPL procurará os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL para SPL é */var/opt/SnapCenter/spl/etc/crl*.

Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo spl.properties contra 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.

Ative certificados de CA para plug-ins

Você deve configurar os certificados de CA e implantar os certificados de CA no servidor SnapCenter e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

Antes de começar

- Você pode ativar ou desativar os certificados de CA usando o cmdlet RUN *Set-SmCertificateSettings*.
- Você pode exibir o status do certificado para os plug-ins usando as *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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Passos

1. No painel de navegação esquerdo, clique em **hosts**.
2. Na página hosts, clique em **hosts gerenciados**.
3. Selecione um ou vários hosts de plug-in.
4. Clique em **mais opções**.
5. Selecione **Ativar Validação de certificado**.

Depois de terminar

O host de guia hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o servidor SnapCenter e o host do plug-in.

- * * Indica que o certificado da CA não está habilitado nem atribuído ao host do plug-in.
- * * Indica que o certificado da CA foi validado com êxito.
- * * Indica que o certificado da 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 são concluídas com êxito.

Instale o plug-in do SnapCenter para VMware vSphere

Se seu banco de dados ou sistema de arquivos estiver armazenado em máquinas virtuais (VMs) ou se você quiser proteger VMs e datastores, você deverá implantar o plug-in do SnapCenter para o dispositivo virtual VMware vSphere.

Para obter informações sobre como implantar, "Visão geral da implantação" consulte .

Implantar certificado CA

Para configurar o certificado CA com o plug-in SnapCenter para VMware vSphere, "Criar ou importar certificado SSL" consulte .

Configure o arquivo CRL

O plug-in do SnapCenter para VMware vSphere procura os arquivos CRL em um diretório pré-configurado. O diretório padrão dos arquivos CRL para o plug-in do SnapCenter para 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, clone ou restauração, você deve configurar o ambiente. Você também pode configurar o servidor SnapCenter para usar a tecnologia SnapMirror e SnapVault.

Para aproveitar as tecnologias SnapVault e SnapMirror, você deve configurar e inicializar uma relação 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 servidor SnapCenter e executar as tarefas de pré-requisito.

- Instalar e configurar o servidor SnapCenter. "Saiba mais"

- Configure o ambiente SnapCenter adicionando conexões do sistema de storage. "Saiba mais"

> O SnapCenter não é compatível com vários SVMs com o mesmo nome em clusters diferentes. Cada SVM registrado no SnapCenter usando o Registro da SVM ou o Registro de cluster precisa ser único.

- Adicione hosts, instale os plug-ins e descubra os recursos.
- Se você estiver usando o servidor SnapCenter para proteger sistemas de arquivos Unix que residem em LUNs ou VMDKs do VMware RDM, você deve implantar o plug-in do SnapCenter para VMware vSphere e Registrar o plug-in com o SnapCenter.
- Instale o Java em seu host Linux.
- Configure o SnapMirror e o SnapVault no ONTAP, se você quiser replicação de backup.

Faça backup de sistemas de arquivos Unix

Descubra os sistemas de arquivos UNIX disponíveis para backup

Depois de instalar o plug-in, todos os sistemas de arquivos nesse host são automaticamente descobertos 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 servidor SnapCenter, 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 plug-in do SnapCenter para VMware vSphere e Registrar o plug-in com o SnapCenter.

  Para obter mais informações, "Implante o plug-in do SnapCenter para VMware vSphere"consulte .

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 juntamente com informações como tipo, nome do host, grupos e políticas de recursos 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 o grupo de recursos que deseja fazer backup. Uma política de backup é um conjunto de regras que regem como você gerencia, agenda e retém backups. Você também pode especificar as configurações de replicação, script e tipo de backup. A criação de uma política economiza tempo quando

você deseja reutilizar a política em outro recurso ou grupo de recursos.

Antes de começar

- Você precisa se preparar para a proteção de dados concluindo tarefas como instalar o SnapCenter, adicionar hosts, descobrir os sistemas de arquivos e criar conexões do sistema de storage.
- Se você estiver replicando snapshots em um storage secundário de espelhamento ou cofre, o administrador do SnapCenter deverá ter atribuído as SVMs a você para os volumes de origem e destino.
- Reveja os pré-requisitos e limitações específicos da sincronização ativa do SnapMirror. Para obter informações, "Limites de objetos para sincronização ativa do SnapMirror" consulte .

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **políticas**.
3. Selecione **Unix File Systems** na lista suspensa.
4. Clique em **novo**.
5. Na página Nome, insira o nome e a descrição da política.
6. Especifique a frequência da programação selecionando **on demand**, **Hourly**, **Daily**, **Weekly** ou **Monthly**.
7. Na página retenção, 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 instantâneos	Selecione **Total de cópias Snapshot a manter** e especifique o número de capturas instantâneas que deseja manter. Se o número de instantâneos exceder o número especificado, os instantâneos serão excluídos com as cópias mais antigas excluídas primeiro. O valor máximo de retenção é 1018 para recursos no ONTAP 9.4 ou posterior e 254 para recursos no ONTAP 9.3 ou anterior. Os backups falharão se a retenção for definida para um valor maior do que o que a versão subjacente do ONTAP suporta. Você deve definir a contagem de retenção como 2 ou superior, se quiser habilitar a replicação do SnapVault. Se você definir a contagem de retenção como 1, a operação de retenção poderá falhar porque o primeiro snapshot é o snapshot de referência para a relação SnapVault até que um snapshot mais recente seja replicado para o destino.
Mantenha as capturas instantâneas por um determinado número de dias	Selecione **manter cópias Snapshot para** e especifique o número de dias para os quais deseja manter as capturas instantâneas antes de excluí-las.

Você pode reter backups de log de arquivamento somente se tiver selecionado os arquivos de log de arquivamento como parte do backup.

8. Na página replicação, especifique as configurações de replicação:

Para este campo…	Faça isso…
Atualize o SnapMirror depois de criar uma cópia Snapshot local	Selecione este campo para criar cópias espelhadas dos conjuntos de backup em outro volume (replicação SnapMirror). Esta opção deve estar ativada para a sincronização ativa do SnapMirror.
Atualize o SnapVault depois de criar uma cópia Snapshot local	Selecione esta opção para executar a replicação de backup disco a disco (backups SnapVault).

Para este campo…	Faça isso…
Etiqueta de política secundária	Selecione uma etiqueta Snapshot. Dependendo do rótulo de captura instantânea selecionado, o ONTAP aplica a política de retenção de snapshot secundária que corresponde ao rótulo. Se você selecionou **Atualizar SnapMirror depois de criar uma cópia Snapshot local**, você pode especificar opcionalmente o rótulo de política secundária. No entanto, se você selecionou **Atualizar SnapVault depois de criar uma cópia Snapshot local**, especifique o rótulo de política secundária.
Contagem de tentativas de erro	Introduza o número máximo de tentativas de replicação que podem ser permitidas antes de a operação parar.

Você deve configurar a política de retenção do SnapMirror no ONTAP para o storage secundário para evitar atingir o limite máximo de snapshots no storage secundário.

9. Na página Script, insira o caminho e os argumentos do prescritor ou postscript que você deseja executar antes ou depois da operação de backup, respetivamente.

   Você deve verificar se os comandos existem na lista de comandos disponível no host plug-in do caminho _ /opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config_.

   Você também pode especificar o valor de tempo limite do script. O valor padrão é de 60 segundos.

10. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas para sistemas de arquivos Unix

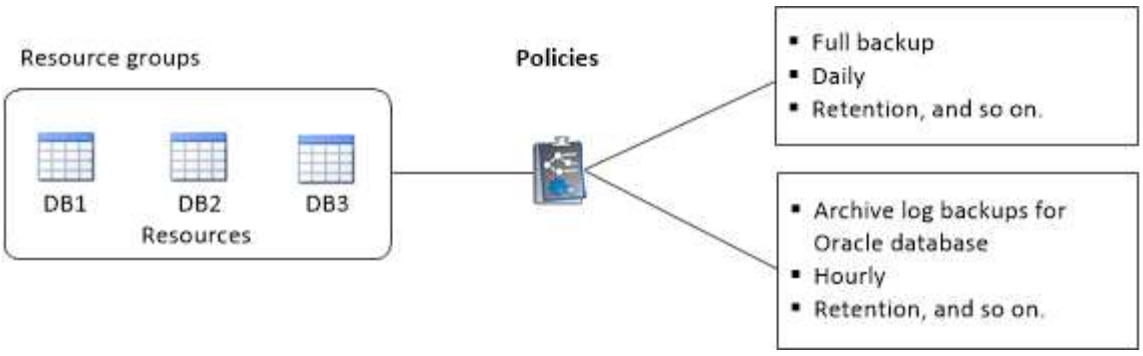
Um grupo de recursos é um contentor onde você adiciona recursos que deseja fazer backup e proteger. Um grupo de recursos permite fazer backup de todos os dados associados aos sistemas de arquivos.

Sobre esta tarefa

- Um banco de dados com arquivos em grupos de discos ASM deve estar no estado "MOUNT" 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 tarefa de proteção de dados que deseja executar.

  A imagem a seguir ilustra a relação entre recursos, grupos de recursos e políticas para bancos de dados:



- Para políticas habilitadas para o SnapLock, para ONTAP 9.12,1 e versões abaixo, se você especificar um período de bloqueio do Snapshot, os clones criados a partir dos snapshots à prova de violação como parte da restauração herdarão o tempo de expiração do SnapLock. O administrador do storage deve limpar manualmente os clones após o tempo de expiração do SnapLock.
- A adição de novos sistemas de arquivos sem a sincronização ativa do SnapMirror a um grupo de recursos existente que contenha recursos com a sincronização ativa do SnapMirror não é suportada.
- A adição de novos sistemas de arquivos a um grupo de recursos existente no modo failover da sincronização ativa do SnapMirror não é suportada. Você pode adicionar recursos ao grupo de recursos apenas no estado regular ou de failback.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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. Introduza um nome para o grupo de recursos no campo Nome.

      O nome do grupo de recursos não deve exceder 250 carateres.

   b. Insira um ou mais rótulos no campo Tag para ajudá-lo a pesquisar o grupo de recursos mais tarde.

      Por exemplo, se você adicionar HR como uma tag a vários grupos de recursos, poderá encontrar mais tarde todos os grupos de recursos associados à tag HR.

   c. Marque a caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

      Por exemplo, customtext_resource group_policy_hostname ou resource group_hostname. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.
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 êxito. Se você tiver adicionado recursos recentemente, eles aparecerão na lista de recursos disponíveis somente depois de atualizar sua lista de recursos.
5. Selecione os recursos na seção recursos disponíveis e mova-os para a seção recursos selecionados.
6. Na página Configurações do aplicativo, execute o seguinte:
   - Selecione a seta Scripts e insira os comandos pre e POST para operações quiesce, Snapshot e unquiesce. Também pode introduzir os pré comandos a serem executados antes de sair em caso de

falha.

- Selecione uma das opções de consistência de backup:
  - Selecione **sistema de arquivos consistente** se você quiser garantir que os dados em cache dos sistemas de arquivos sejam limpos antes de criar o backup e nenhuma operação de entrada ou saída seja permitida no sistema de arquivos durante a criação do backup.

    Para o sistema de arquivos consistente, instantâneos de grupo de consistência serão feitos para LUNs envolvidos no grupo volume.

  - Selecione **Crash consistente** se quiser garantir que os dados em cache dos sistemas de arquivos sejam limpos antes de criar o backup.

    Se você adicionou 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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

   c. Na janela Adicionar programações para a política *policy_name*, configure a programação e clique em **OK**.

      Onde, *policy_name* é o nome da política selecionada.

      As programações configuradas são listadas na coluna agendas aplicadas.

   As agendas de backup de terceiros não são suportadas quando sobrepõem-se às agendas 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 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-SmtpServer.

9. Revise o resumo e clique em **Finish**.

Faça backup de sistemas de arquivos Unix

Se um recurso não fizer parte de qualquer grupo de recursos, você poderá fazer backup do recurso na página recursos.

Passos

1. No painel de navegação esquerdo, selecione **Resources** e o plug-in apropriado na lista.
2. Na página recursos, selecione **caminho** na lista Exibir.
3. Clique em e selecione o nome do host e os sistemas de arquivos Unix para filtrar os recursos.
4. Selecione o sistema de ficheiros que pretende efetuar uma cópia de segurança.
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 da captura Instantânea.

      Por exemplo, `customtext_policy_hostname` ou `resource_hostname`. Por padrão, um carimbo de data/hora é anexado ao nome do instantâneo.

6. Na página Configurações do aplicativo, execute o seguinte:
   - Selecione a seta Scripts e insira os comandos pre e POST para operações quiesce, Snapshot e unquiesce. Também pode introduzir os pré comandos a serem executados antes de sair em caso de falha.
   - Selecione uma das opções de consistência de backup:
     - Selecione **File System consistent** se quiser garantir que os dados em cache dos sistemas de arquivos sejam limpos antes de criar o backup e nenhuma operação seja executada no sistema de arquivos enquanto cria o backup.
     - Selecione **Crash consistente** se quiser garantir que os dados em cache dos sistemas 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 agendas para políticas selecionadas, as políticas selecionadas são listadas.

   b. Clique na coluna Configurar agendas para configurar uma agenda para a política desejada.
   c. Na janela Adicionar agendas para a política *policy_name* , configure a programação e `OK` selecione .

      policy_name é o nome da política selecionada.

   As programações configuradas são listadas na coluna agendas aplicadas.

8. Na página notificação, selecione os cenários em que você deseja enviar os e-mails da 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 quiser anexar o relatório da operação de backup realizada no recurso, selecione **Anexar Relatório de**

trabalho.

> Para notificação por e-mail, você deve ter especificado os detalhes do servidor SMTP usando o comando GUI ou PowerShell `Set-SmSmtpServer` .

9. Revise o resumo e clique em **Finish**.

   A página de topologia é exibida.

10. Clique em **fazer backup agora**.
11. Na página Backup, execute as seguintes etapas:
    a. Se você tiver aplicado 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. Monitorize o progresso da operação clicando em **Monitor** > **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 uma programação configurada, os backups serão criados de acordo com a programação.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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 em 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. Monitorize o progresso selecionando **Monitor > trabalhos**.

Monitorar backup de sistemas de arquivos Unix

Saiba como monitorar o progresso das operações de backup e operações de 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. Você pode querer verificar o progresso para determinar quando ele está concluído ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado correspondente das operações:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- 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 a que apenas as operações de cópia de segurança sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Backup**.
   d. Na lista suspensa **Status**, selecione o status da cópia de segurança.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione um trabalho de cópia de segurança e clique em **Detalhes** para ver os detalhes do trabalho.

   Embora o status do trabalho de backup seja exibido , quando você clica nos detalhes do trabalho, você pode ver que algumas das tarefas secundárias da operação de backup ainda estão em andamento ou marcadas com sinais de aviso.

5. Na página Detalhes da tarefa, clique em **Exibir logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Monitore operações de proteção de dados no painel atividade

O painel atividade exibe as cinco operações mais recentes executadas. O painel atividade também é exibido quando a operação foi iniciada e o status da operação.

O painel atividade exibe informações sobre operações de backup, restauração, clone e backup agendadas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 da tarefa**.

Veja sistemas de arquivos Unix protegidos na página topologia

Ao se preparar para fazer backup, restauração ou clone de um recurso, talvez seja útil exibir uma representação gráfica de todos os backups, sistemas de arquivos restaurados e clones no storage primário e secundário.

Sobre esta tarefa

Na página topologia, você pode ver todos os backups, sistemas de arquivos restaurados e clones disponíveis para o grupo de recursos ou recursos selecionado. Você pode visualizar os detalhes desses backups, sistemas de arquivos restaurados e clones e, em seguida, selecioná-los para executar operações de proteção de dados.

Você pode revisar os ícones a seguir na exibição Gerenciar cópias para determinar se os backups e clones estão disponíveis no storage primário ou secundário (cópias espelhadas ou cópias do Vault).

- exibe o número de backups e clones disponíveis no storage primário.
- Exibe o número de backups e clones espelhados no storage secundário usando a tecnologia SnapMirror.
- Exibe o número de backups e clones replicados no storage secundário usando a tecnologia SnapVault.

  O número de backups exibidos inclui os backups excluídos do armazenamento secundário. Por exemplo, se você criou backups 6 usando uma política para reter apenas 4 backups, o número de backups exibidos é 6.

> Os clones de um backup de um espelhamento flexível de versão em um volume do tipo cofre-espelho são exibidos na visualização de topologia, mas a contagem de backup espelhado na visualização de topologia não inclui o backup flexível de versão.

Se você tiver uma relação secundária como sincronização ativa do SnapMirror (lançada inicialmente como SnapMirror Business Continuity [SM-BC]), você poderá ver os seguintes ícones adicionais:

- O site da réplica está em cima.

- O site da réplica está inativo.
- A relação do espelho secundário ou do cofre não foi restabelecida.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o recurso ou o 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 é exibida.

4. Revise o cartão de resumo para ver um resumo do número de backups e clones disponíveis no storage primário e secundário.

   A seção cartão de resumo exibe o número total de backups e clones.

   Clicar no botão **Refresh** inicia uma consulta do armazenamento para exibir uma contagem precisa.

   Se o backup habilitado para SnapLock for feito, clique no botão **Atualizar** atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP. Um horário semanal também atualiza o tempo de expiração do SnapLock primário e secundário recuperado do ONTAP.

   Quando o sistema de arquivos é espalhado por vários volumes, o tempo de expiração do SnapLock para o backup será o tempo de expiração do SnapLock mais longo definido para um instantâneo em um volume. O tempo de expiração mais longo do SnapLock é recuperado do ONTAP.

   Para a 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 a relação de sincronização ativa do SnapMirror.

   - Para a sincronização ativa do SnapMirror e somente para o ONTAP 9.14,1, as relações de espelhamento do Async ou EspelrorVault do Async com o novo destino primário devem ser configuradas manualmente após o failover. A partir do ONTAP 9.15,1 em diante, o espelho do Async ou o MirrorVault do Async 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 **Refresh** somente depois que um backup tiver sido criado.
5. No modo de 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 um 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 estão no armazenamento secundário.

7. Se quiser excluir um clone, selecione-o na tabela e clique em .

Exemplo mostrando backups e clones no storage primário

Restaurar e recuperar sistemas de arquivos Unix

Restaure 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 servidor SnapCenter, listar os backups e 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*. Em alternativa, pode também 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 no local principal.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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** nos sistemas de armazenamento primário ou secundário (espelhado ou replicado).
5. Selecione a cópia de segurança na tabela e, em seguida, clique em * .
6. Na página Restaurar escopo:
   - Para sistemas de arquivos NFS, por padrão, a opção **Connect and Copy** Restore está selecionada. Você também pode selecionar **Reverter volume** ou **Restauração rápida**.
   - Para sistemas de arquivos que não sejam NFS, o escopo de restauração é selecionado dependendo do layout.

     Os novos ficheiros criados após a cópia de segurança poderão não estar disponíveis após a restauração, dependendo do tipo de sistema de ficheiros e do esquema.
7. Na página PreOps, insira os comandos de pré-restauração a serem executados antes de executar uma tarefa de restauração.
8. Na página PostOps, insira os comandos pós-restauração para 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 caminho */opt/NetApp/SnapCenter/scc/etc/allowed_Commands.config*.
9. Na página notificação, na lista suspensa **preferência de e-mail**, selecione os cenários em que 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 pretender anexar o relatório da operação de restauro efetuada, tem de selecionar **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-SmtpServer.
10. Revise o resumo e clique em **Finish**.

    Se a operação de restauração falhar, a reversão não é suportada.

    Em caso de restauração de um sistema de arquivos residente no 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 padrão do sistema de arquivos NFS.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Monitorar operações de restauração de sistemas de arquivos Unix

Pode monitorizar o progresso de diferentes operações de restauro do SnapCenter utilizando a página trabalhos. Você pode querer verificar o progresso de uma operação

para determinar quando ela está concluída ou se há um 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 executar.

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista de modo que apenas as operações de restauração sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Restore**.
   d. Na lista suspensa **Status**, selecione o status de restauração.
   e. Clique em **Apply** para ver as operações que foram concluídas com sucesso.
4. Selecione o trabalho de restauração e clique em **Detalhes** para exibir os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Visualizar logs**.

   O botão **View logs** exibe os logs detalhados para a operação selecionada.

Clonar sistemas de arquivos Unix

Clone 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 ignorar a atualização do arquivo fstab definindo o valor de *SKIP_FSTAB_UPDATE* para **true** no arquivo *agent.properties* localizado em */opt/NetApp/SnapCenter/scc/etc*.
- Você pode ter um nome de volume de clone estático e caminho de junção definindo o valor de *USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT* para **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 esta propriedade o nome do volume do clone e o caminho de junção serão como <Source_volume_name>_Clone_<Timestamp>, mas agora será <Source_volume_name>_Clone_<Clone_Name>

Isso mantém o nome constante para que você possa manter manualmente o arquivo fstab atualizado se você não preferir atualizar o fstab pelo SnapCenter.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 de cópias locais (primárias), cópias espelhadas (secundárias) ou cópias do Vault (secundárias).
5. Selecione a cópia de segurança na tabela e, em seguida, 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 clone	Especifique o caminho onde o sistema de arquivos será montado.

7. Na página Scripts, execute as seguintes etapas:
   a. Digite os comandos para pré-clone ou pós-clone que devem ser executados antes ou depois da operação clone, respetivamente.

   > Você deve verificar se os comandos existem na lista de comandos disponível no host plug-in do 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 quiser anexar o relatório da operação clone executada, 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-SmtpServer.

9. Revise o resumo e clique em **Finish**.
10. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Divida um clone

Você pode usar o SnapCenter para dividir um recurso clonado do recurso pai. O clone

que é dividido torna-se independente do recurso pai.

Sobre esta tarefa

- Não é possível executar a operação de divisão de clones em um clone intermediário.

  Por exemplo, depois de criar clone1 a partir de um backup de banco de dados, você pode criar um backup de clone1 e clonar esse backup (clone2). Depois de criar o clone2, o clone1 é um clone intermediário e não é possível executar a operação de divisão de clones no clone1. No entanto, você pode executar a operação de divisão de clones no clone2.

  Depois de dividir clone2, você pode executar a operação de divisão de clones no clone1 porque clone1 não é mais o clone intermediário.

- Quando você divide um clone, as cópias de backup e as tarefas de clone do clone são excluídas.
- Para obter informações sobre limitações de operação de divisão de clones, "Guia de gerenciamento de storage lógico do ONTAP 9" consulte .
- Certifique-se de que o volume ou o agregado no sistema de storage esteja on-line.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página **recursos**, selecione a opção apropriada na lista Exibir:

Opção	Descrição
Para aplicativos 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 do recurso é exibida.

4. No modo de 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 deve ser dividido e o espaço necessário disponível no agregado e clique em **Iniciar**.
6. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

   A operação de divisão de clones deixa de responder se o serviço SMCore for reiniciado. Você deve executar o cmdlet Stop-SmJob para interromper a operação de divisão de clones e tentar novamente a operação de divisão de clones.

   Se você quiser um tempo de enquete mais longo 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 que o SMCore busque o status da operação de divisão de clones. O valor é em milissegundos e o valor padrão é de 5 minutos.

   Por exemplo:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

A operação de inicialização dividida de clone falhará se o backup, a restauração ou outra divisão de clones estiver em andamento. Você deve reiniciar a operação de divisão de clones somente depois que as operações em execução estiverem concluídas.

Informações relacionadas

"O clone ou a verificação do SnapCenter falha com o agregado não existe"

Monitorar operações de clones de sistemas de arquivos Unix

Você pode monitorar o andamento das operações de clone do SnapCenter usando a página tarefas. Você pode querer verificar o progresso de uma operação para determinar quando ela está concluída ou se há um problema.

Sobre esta tarefa

Os seguintes ícones são apresentados na página trabalhos e indicam o estado da operação:

- Em curso
- Concluído com êxito
- Falha
- Preenchido com avisos ou não foi possível iniciar devido a avisos
- Em fila de espera
- Cancelado

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **empregos**.
3. Na página **trabalhos**, execute as seguintes etapas:
   a. Clique para filtrar a lista para que apenas operações de clone sejam listadas.
   b. Especifique as datas de início e fim.
   c. Na lista suspensa **Type**, selecione **Clone**.
   d. Na lista suspensa **Status**, selecione o status do clone.
   e. Clique em **Apply** para ver as operações concluídas com êxito.
4. Selecione a tarefa clone e clique em **Detalhes** para exibir os detalhes da tarefa.
5. Na página Detalhes da tarefa, clique em **Exibir logs**.

Proteja aplicativos em execução no Azure NetApp Files

Proteja aplicativos em execução no Azure NetApp Files

O SnapCenter é compatível com a proteção de aplicações como Oracle, SQL e SAP HANA que residem no Azure NetApp Files. A partir da versão 6.0.1, o SnapCenter dá suporte ao recurso de backup Azure NetApp Files que expande os recursos de proteção de dados do Azure NetApp Files fornecendo solução de backup totalmente gerenciada para recuperação, arquivamento e conformidade de longo prazo.

O Azure NetApp Files é uma solução de storage premium que pode ser cara para a retenção de backup a longo prazo. Para otimizar custos, você pode migrar os backups do storage Azure NetApp Files para um armazenamento de objetos Azure. A partir do SnapCenter 6,0.1, é possível fazer backup e clonar aplicativos que residem no Azure NetApp Files para o armazenamento de Blobs do Azure (armazenamento de objetos). Você pode manter duas cópias dos seus dados, cópias snapshot de volume no storage Azure NetApp Files para recuperação de curto prazo e outra cópia no armazenamento Blob do Azure para recuperação de longo prazo.

Quando uma política com backup do Azure NetApp Files está habilitada e associada a um recurso, o SnapCenter manipula a criação de snapshots de volume e o backup no armazenamento de Blobs do Azure. O SnapCenter cria o cofre de backup e habilita o backup para o volume. Se você ativou o backup para o volume, o SnapCenter utiliza o cofre existente.

Limitações

- As funcionalidades de armazenamento de objetos para sistemas de armazenamento FAS ou AFF ONTAP e FSxN não são suportadas.
- Os workflows de montagem e catálogo do Oracle e SAP HANA não são compatíveis com backups de storage de objetos, mas são compatíveis com snapshots.
- Os clones do Oracle PDB não são compatíveis com backups de storage de objetos, mas são compatíveis com snapshots.
- A verificação de backup do storage de objetos, suporte à API REST, gerenciamento do ciclo de vida de clones do storage de objetos e recursos de geração de relatórios para backups de storage de objetos não é compatível.
- A restauração de backups no armazenamento de Blobs do Azure para o Azure NetApp Files não é suportada. Você pode usar a opção clone, alternativamente.
- Divisão de clones não é suportada.

Instale o SnapCenter e crie credenciais

Instale o SnapCenter na Máquina Virtual do Azure

Você pode baixar o software SnapCenter 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 de instalação do servidor SnapCenter. Para obter informações, "Prepare-se para instalar o servidor SnapCenter"consulte .
- Se você é novo no Azure NetApp Files e não tem uma conta NetApp existente, certifique-se de que se registrou para que você possa acessar o software SnapCenter.

Passos

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

   Depois de iniciar a instalação, todas as pré-verificações são executadas e, se os requisitos mínimos não forem atendidos, as mensagens de erro ou aviso apropriadas serão exibidas. Você pode ignorar as mensagens de aviso e prosseguir com a instalação; no entanto, os erros devem ser corrigidos.

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

   Você não precisa especificar a senha para o banco de dados do repositório do MySQL Server. Durante a instalação do servidor SnapCenter, 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 quaisquer valores inválidos, as mensagens de erro apropriadas serão exibidas. Deve voltar a introduzir os valores e, em seguida, iniciar a instalação.

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

   No entanto, se você clicar em **Cancelar** quando as operações "SnapCenter Server site Restart" ou "Waiting for SnapCenter Server to start" estiverem sendo executadas, a instalação continuará sem cancelar a operação.

Registre o produto para habilitar o suporte

Se você é novo no NetApp e não tem uma conta NetApp existente, deve Registrar o produto para habilitar o suporte.

Passos

1. Depois de 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.comem .
4. Clique em **Eu não sou um Cliente NetApp registrado**.
5. Especifique os seus dados para se registar.
6. Deixe o campo NetApp Reference SN em branco.
7. Selecione **SnapCenter** na lista suspensa linha de produtos.

8. Selecione o fornecedor de faturação.
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 criar a credencial do Azure, certifique-se de que criou o principal de serviço no Azure. O ID do locatário, o ID do cliente e a chave secreta associados ao responsável do serviço serão necessários para criar a credencial do Azure.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página Configurações, clique em **Credential**.
3. Clique em **novo**.
4. Na página Credential (credencial), especifique as seguintes informações necessárias para criar a credencial.

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para a credencial.
Modo de autenticação	Selecione **credencial do Azure** na lista suspensa.
ID do inquilino	Insira o ID do locatário.
ID do cliente	Introduza a ID do cliente.
Chave secreta do cliente	Introduza a chave secreta do cliente.

5. Clique em **OK**.

Configure 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 a ID da subscrição, a credencial do Azure e a conta do Azure NetApp.

As licenças padrão e a licença baseada em capacidade não são necessárias para o Azure NetApp Files.

Passos

1. No painel de navegação esquerdo, clique em **Storage Systems**.
2. Na página sistemas de armazenamento, selecione **Azure NetApp Files** e clique em **novo**.

3. Selecione a credencial, a ID da assinatura e a conta do NetApp nas respetivas 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 **Credential**.
3. Clique em **novo**.
4. Na página Credential (credencial), especifique as seguintes informações necessárias para criar a credencial.

Para este campo…	Faça isso…
Nome da credencial	Introduza um nome para a credencial.
Modo de autenticação	Selecione o modo de autenticação na lista pendente.
Tipo de autenticação	Selecione **baseado em senha** ou **baseado em chave SSH** (somente para host Linux).
Nome de utilizador	Especifique o nome de usuário.
Palavra-passe	Se tiver selecionado a autenticação baseada na palavra-passe, especifique a palavra-passe.
Chave privada SSH	Se você selecionou a autenticação baseada em chave SSH, especifique a chave privada.
Use sudo Privileges	Marque a caixa de seleção usar sudo Privileges se estiver criando credenciais para um usuário que não seja root. Isso é aplicável apenas para usuários Linux.

5. Clique em **OK**.

Proteger bancos de dados SAP HANA

Adicione hosts e instale o plug-in do SnapCenter para 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 as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host.
- Se você estiver instalando no host centralizado, verifique se o software cliente SAP HANA está instalado nesse host e abra as portas necessárias no host de 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 **Add**.
4. Na página hosts, execute as seguintes ações:
   a. No campo Host Type (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 instalar.
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 **Confirm and Submit**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós no cluster.

9. Monitorize 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 detecção automática não é compatível com a configuração de vários host HANA, ela precisa ser adicionada somente por meio de plug-in centralizado.

Passos

1. No painel de navegação à esquerda, selecione o plug-in do 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 contentor único, recipiente de banco de dados multitenant ou volume não-dados.
   b. Introduza o nome do sistema SAP HANA.
   c. Introduza a ID do sistema (SID).
   d. Selecione o host do plug-in.
   e. Digite a chave para se conetar ao sistema SAP HANA.
   f. Introduza o nome de utilizador para o qual a chave de armazenamento de utilizador seguro HDB está configurada.
4. Na página fornecer espaço físico 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 **Finish**.

Criar políticas de backup para bancos de dados SAP HANA

Antes de usar o SnapCenter para fazer backup dos recursos do banco de dados do SAP HANA, você precisa 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 **File-based** (baseado em ficheiros) se pretender efetuar uma verificação de integridade da base de dados.
   c. Selecione **Snapshot based** se quiser criar um backup usando a tecnologia Snapshot.
6. Na página Snapshot e backup, execute as seguintes etapas:
   a. Selecione a frequência da cópia de segurança agendada.
   b. Especifique as definições de retenção.
   c. Se você quiser habilitar o backup do Azure NetApp Files, selecione **Ativar backup** e especifique as configurações de retenção.
7. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas de backup do SAP HANA

Um grupo de recursos é o contentor ao qual você deve adicionar recursos que deseja fazer backup e proteger.

Um grupo de recursos permite fazer 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 tarefa de proteção de dados que deseja executar.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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	Introduza um nome para o grupo de recursos.
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos.
Use o formato de nome personalizado para cópia Snapshot	Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

4. Na página recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Resource Type**.
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 agendas, clique em + para a política que deseja configurar.
   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação 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 **Finish**.

Fazer backup de bancos de dados SAP HANA executados no Azure NetApp Files

Se um recurso ainda não fizer parte de qualquer grupo de recursos, você poderá fazer backup do recurso na página recursos.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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 **Use o formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.
5. Na página Configurações do aplicativo, faça o seguinte:
   a. Selecione a seta **backups** para definir opções de backup adicionais.
   b. Selecione a seta **Scripts** para executar comandos pré e POST para operações quiesce, Snapshot e unquiesce.
   c. Selecione a seta **Custom Configurations** (Configurações personalizadas) e, em seguida, insira os pares de valores personalizados necessários para todos os trabalhos que utilizam este recurso.
   d. Selecione a ferramenta **cópia Snapshot > SnapCenter sem consistência do sistema de arquivos** para criar snapshots.

      A opção **consistência do sistema de arquivos** é aplicável apenas 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 agendas para a política para a qual você deseja configurar um agendamento.
   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e selecione **OK**.

      policy_name é o nome da política selecionada.

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 **Finish**.
9. Selecione **fazer uma cópia de segurança 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 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. Monitorize o progresso da operação clicando em **Monitor** > **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 **Resources** 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 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. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Restaure e recupere bancos de dados do SAP HANA

Você pode restaurar e recuperar dados dos backups.

Sobre esta tarefa

Para sistemas HANA detetados automaticamente, se a opção **recurso completo** estiver selecionada, a restauração será executada usando a tecnologia de restauração de snapshot de Arquivo único. Se a caixa de seleção **Fast Restore** estiver selecionada, a tecnologia volume Revert será usada.

Para recursos adicionados manualmente, a tecnologia de reversão de volume é sempre usada.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre 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** nos sistemas de armazenamento primário ou secundário (espelhado ou abobadado).
5. Na tabela de backup principal, selecione o backup do qual você deseja restaurar e clique em * * .
6. Na página Restaurar escopo, selecione **recurso completo**.

   Todos os volumes de dados configurados do banco de dados SAP HANA são restaurados.

7. Para sistemas HANA detetados automaticamente, na página escopo de recuperação, execute as

seguintes ações:

a. Selecione **Recover to most recent State** (recuperar para o estado mais recente) se pretender recuperar o mais próximo possível da hora atual.

b. Selecione **Recover to Point in Time** se você quiser recuperar para o ponto especificado no tempo.

c. Selecione **Recover to specified data backup** se você quiser recuperar para um backup de dados específico.

d. Selecione **sem recuperação** se não quiser recuperar agora.

e. Especifique as localizações de cópia de segurança do registo.

f. Especifique o local do catálogo de backup.

8. Na página operações anteriores, insira pré-restauração e desmonte comandos para serem executados antes de executar um trabalho de restauração.
9. Na página Post OPS, insira os comandos mount e POST Restore para serem executados após a execução de 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 **Finish**.
12. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Clone o backup do 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 espessos e são criados no pool de capacidade pai.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, filtre recursos da lista suspensa **Exibir** com base no tipo de recurso.
3. Selecione o grupo de recursos ou recursos.
4. Na exibição Gerenciar cópias, selecione **backups** no sistema de armazenamento primário.
5. Selecione o backup de dados na 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.

    Ele pode ser um host plug-in centralizado ou um host de sistema HANA.

> Se o plug-in HANA for instalado em um host centralizado que gerencia bancos de DADOS HANA em outros hosts, ao criar ou excluir clones, o SnapCenter descartará intencionalmente 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 pré ou pós-clone para executar operações de montagem e desmontagem.

a. Insira o SID do SAP HANA para clonar dos backups existentes.

b. Insira endereços IP ou os nomes de host nos quais os volumes clonados serão exportados.

c. Se os volumes de ANF do banco de dados SAP HANA estiverem configurados em um pool de CAPACIDADE DE QOS manual, especifique a QOS para os volumes clonados.

Se A QOS para os volumes clonados não for especificada, a QOS do volume de origem será usada. 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. Digite os comandos para pré-clone ou pós-clone que devem ser executados antes ou depois da operação clone, respetivamente.

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 de host de destino clone for instalado no host SAP HANA, o SnapCenter removerá automaticamente os volumes de DADOS HANA existentes no host clone de destino 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 **Finish**.

10. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

O clone Split está desativado para clones do ANF porque o clone do ANF já é um volume independente criado a partir do Snapshot selecionado.

Proteja bancos de dados Microsoft SQL Server

Adicione hosts e instale o plug-in do SnapCenter para o banco de dados SQL Server

O SnapCenter é compatível com a proteção de dados de instâncias SQL em compartilhamentos SMB no Azure NetApp Files. As configurações do grupo de disponibilidade e independente (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 as permissões de instalação e desinstalação do plug-in, como a função Administrador do SnapCenter.
- Ao instalar um plug-in em um host do Windows, se você especificar uma credencial que não está integrada ou se o usuário pertence a um usuário local do grupo de trabalho, será necessário desativar o UAC no host.

Passos

1. No painel de navegação esquerdo, selecione **hosts**.
2. Verifique se a guia **hosts gerenciados** está selecionada na parte superior.

3. Selecione **Adicionar**.
4. Na página hosts, faça o seguinte:
   a. No campo Host Type (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 **Select Plug-ins to Install**, selecione os plug-ins a instalar.
6. (Opcional) clique em **mais Opções** e especifique os detalhes.
7. Selecione **Enviar**.
8. Selecione **Configure log Directory** e, na página Configurar diretório de log do host, insira o caminho SMB do diretório de log do host e clique em **Save**.
9. Clique em **Submit** e monitore o progresso da instalação.

Criar políticas de backup para bancos de dados do SQL Server

Você pode criar uma política de backup para o recurso ou para o grupo de recursos antes de usar o SnapCenter para fazer backup de recursos do SQL Server ou criar uma política de backup no momento em que criar um grupo de recursos ou fazer 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 cópia de segurança.
      i. Selecione **Backup completo e Log Backup** 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 **Log Backup** se quiser fazer backup apenas dos logs de transação.
      iv. Selecione **Backup somente cópia** se quiser fazer backup de seus recursos usando outro aplicativo.
   c. Na seção Configurações do Grupo de disponibilidade, execute as seguintes ações:
      i. Selecione cópia de segurança na réplica de cópia de segurança preferida se pretender efetuar uma cópia de segurança apenas na réplica.
      ii. Selecione a réplica AG primária ou a réplica AG secundária para o backup.
      iii. Selecione a prioridade da cópia de segurança.
6. Na página Snapshot e backup, execute as seguintes etapas:
   a. Selecione a frequência da cópia de segurança agendada.

b. Especifique as configurações de retenção dependendo do tipo de backup selecionado.

c. Se você quiser habilitar o backup do Azure NetApp Files, selecione **Ativar backup** e especifique as configurações de retenção.

7. Na página Verificação, execute as seguintes etapas:

a. Na seção Executar verificação para as seguintes programações de backup, selecione a frequência de agendamento.

b. Na seção Opções de verificação consistência de banco de dados, execute as seguintes ações:

i. Selecione **Limit 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 para detetar páginas rasgadas, falhas de checksum e falhas comuns de hardware que afetam o banco de dados.

ii. Selecione **suprimir todas as mensagens de informação (NO_INFOMSGS)** para suprimir todas as mensagens informativas.

Selecionado por predefinição.

iii. Selecione **Exibir todas as mensagens de erro relatadas por objeto (ALL_ERRORMSGS)** para exibir todos os erros relatados por objeto.

iv. Selecione **não verifique índices não agrupados (NOINDEX)** se você não quiser verificar índices não agrupados.

O banco de dados do SQL Server usa o Microsoft SQL Server Database Consistency Checker (DBCC) para verificar a integridade física e lógica dos objetos no banco de dados.

v. Selecione **Limit as verificações e obtenha os bloqueios em vez de usar uma cópia Snapshot do banco de dados interno (TABLOCK)** para limitar as verificações e obter 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 prescritor ou postscript que devem ser executados antes ou depois da operação de verificação, respetivamente.

8. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas de backup SQL

Um grupo de recursos é o contentor ao qual você deve adicionar recursos que deseja fazer backup e proteger.

Um grupo de recursos permite fazer 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 tarefa de proteção de dados que deseja executar.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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	Introduza um nome para o grupo de recursos.
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos.
Use o formato de nome personalizado para cópia Snapshot	Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.

4. Na página recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Resource Type**.
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 agendas, clique em + para a política que deseja configurar.
   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação 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 pretende configurar o seu agendamento de verificação e, em seguida, clique em * * + .
   c. Selecione **Executar verificação após cópia de segurança** 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 **Finish**.

Faça backup de bancos de dados do SQL Server em execução no Azure NetApp Files

Se um recurso ainda não fizer parte de qualquer 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 Azure Windows não tiver um IP de cluster atribuído ou se não estiver acessível a partir do SnapCenter. O IP do balanceador de carga deve ser configurado e acessível a partir do servidor SnapCenter.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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 **Use o formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.
4. Na página políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Selecione * * na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.
   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e selecione **OK**.

      policy_name é o nome da política selecionada.

   d. Selecione **Use o agendador do Microsoft SQL Server** e, em seguida, selecione a instância do agendador na lista suspensa **Instância do Agendador** que está 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 pretende configurar o seu agendamento de verificação e, em seguida, clique em * * .
   c. Selecione **Executar verificação após cópia de segurança** 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 **Finish**.
8. Selecione **fazer uma cópia de segurança 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 deseja usar para backup.
   b. Selecione **Verify after backup**.
   c. Selecione **Backup**.
10. Monitorize o progresso da operação clicando em **Monitor** > **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 **Resources** 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 deseja usar para backup.
   b. Após o backup, selecione **Verify** para verificar o backup sob demanda.
   c. Selecione **Backup**.
5. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Restaurar e recuperar bancos de dados do SQL Server

Você pode usar o SnapCenter para restaurar bancos de dados do SQL Server com backup. Restauração de 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 de diretório ativo que pertence ao domínio de diretório ADactive SMB 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 diretório ativo com as permissões necessárias.

Se a conta de serviço de serviços de plug-in do SnapCenter não for um usuário de diretório ativo e, ao executar a restauração para um host alternativo, o usuário que tiver o controle total sobre os volumes de origem será necessário para que ele possa ser representado e executar a operação necessária.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 a base de dados ou o grupo de recursos na lista.
4. Na exibição Gerenciar cópias, selecione **backups** no sistema de armazenamento.
5. Selecione a cópia de segurança na tabela e, em seguida, clique no ícone.
6. Na página Restaurar escopo, selecione uma das seguintes opções:
   a. Selecione **Restaurar o banco de dados para o mesmo host onde o backup foi criado** se você quiser restaurar o banco de dados para o mesmo servidor SQL onde os backups são feitos.
   b. Selecione **Restaurar o banco de dados para um host alternativo** se você quiser que o banco de dados seja restaurado para um servidor SQL diferente no mesmo ou em um host diferente onde os backups são feitos.
7. Na página âmbito de recuperação, selecione uma das seguintes opções:
   a. Selecione **nenhum** quando precisar restaurar somente o backup completo sem nenhum log.

b. Selecione **todos os backups de log** operação de restauração de backup atualizada 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 em 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 transação não são aplicados ao banco de dados restaurado.

e. Se tiver selecionado **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-operações e Pós-operações, 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 **Finish**.
11. Monitorize o processo de restauro utilizando a página **Monitor** > **trabalhos**.

Clone 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 espessos e são criados no pool de capacidade pai.

Sobre esta tarefa

Você deve garantir que a instância de destino para clone esteja configurada com um usuário de diretório ativo que pertence ao domínio de diretório SMB ADactive 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 diretório ativo com as permissões necessárias.

Se a conta de serviço de serviços de plug-in do SnapCenter não for um usuário de diretório ativo, então, durante a execução do clone, o usuário que tiver controle total sobre os volumes de origem será necessário para que ele possa ser representado e executar a operação necessária.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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 o grupo de recursos.
4. Na página de exibição **Gerenciar cópias**, selecione o backup do sistema de armazenamento primário.
5. Selecione a cópia de segurança e, em seguida, selecione *.
6. Na página **Clone Options**, forneça todos os detalhes necessários.
7. Na página local, selecione um local de armazenamento para criar um clone.

   Se os volumes do ANF do banco de dados do SQL Server estiverem configurados em um pool de CAPACIDADE DE QOS manual, especifique a QOS para os volumes clonados.

   Se A QOS para os volumes clonados não for especificada, a QOS do volume de origem será usada. 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 você quiser clonar apenas o backup completo sem nenhum log.
   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 você quiser clonar o banco de dados com base nos logs de backup criados até o log de backup com a data selecionada.
   d. Selecione **por data específica até** se você não quiser aplicar os logs de transação após a data e hora especificadas.
9. Na página **Script**, insira o tempo limite do script, o caminho e os argumentos do prescritor ou postscript que devem ser executados antes ou depois da operação clone, respetivamente.
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 **Finish**.
12. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Execute o ciclo de vida do clone

Com o SnapCenter, você pode criar clones de um grupo de recursos ou banco de dados. Você pode executar um clone sob demanda ou agendar operações de clone 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 **Resources** 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 o grupo de recursos.
4. Na página de exibição **Gerenciar cópias**, selecione o backup do sistema de armazenamento primário.
5. Selecione a cópia de segurança e, em seguida, selecione *.
6. Na página **Clone Options**, forneça todos os detalhes necessários.
7. Na página local, selecione um local de armazenamento para criar um clone.

   Se os volumes do ANF do banco de dados do SQL Server estiverem configurados em um pool de CAPACIDADE DE QOS manual, especifique a QOS para os volumes clonados.

   Se A QOS para os volumes clonados não for especificada, a QOS do volume de origem será usada. 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 prescritor ou postscript que devem ser executados antes ou depois da operação clone, respetivamente.
9. Na página Agendar, execute uma das seguintes ações:
   - Selecione **Executar agora** se quiser executar a tarefa clone imediatamente.
   - Selecione **Configurar agendamento** quando quiser determinar com que frequência a operação de clone deve ocorrer, quando a programação de clones deve ser iniciada, em que dia a operação de

clone deve ocorrer, quando a programação deve expirar e se os clones devem ser excluídos após a expiração da programação.

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 **Finish**.
12. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Proteger bancos de dados Oracle

Adicione hosts e instale o plug-in do SnapCenter para o banco de dados Oracle

Você pode usar a página Adicionar host para adicionar hosts e, em seguida, instalar o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do 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 Oracle RAC One Node, você deve instalar o plug-in em 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 **Add**.
4. Na página hosts, execute as seguintes ações:
   a. No campo Host Type (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 instalar.
6. (Opcional) clique em **mais Opções** e especifique os detalhes.
7. Clique em **Enviar**.
8. Verifique a impressão digital e clique em **Confirm and Submit**.

   Em uma configuração de cluster, você deve verificar a impressão digital de cada um dos nós no cluster.

9. Monitorize o progresso da instalação.

Criar políticas de backup para bancos de dados Oracle

Antes de usar o SnapCenter para fazer backup dos recursos do banco de dados Oracle, você deve criar uma política de backup para o recurso ou para o 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. 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 cópia de segurança como cópia de segurança online ou offline.
   c. Se você quiser catalogar o backup usando o Oracle Recovery Manager (RMAN), selecione **Catálogo de backup com o Oracle Recovery Manager (RMAN)**.
   d. Se você quiser podar logs de arquivo após o backup, selecione **Prune archive logs after backup**.
   e. Especifique as definições do registo de eliminação de arquivo.
7. Na página Snapshot e backup, execute as seguintes etapas:
   a. Selecione a frequência da cópia de segurança agendada.
   b. Especifique as definições de retenção.
   c. Se você quiser habilitar o backup do Azure NetApp Files, selecione **Ativar backup** e especifique as configurações de retenção.
8. Na página Script, insira o caminho e os argumentos do prescritor ou postscript que você deseja executar antes ou depois da operação de backup, respetivamente.
9. Na página Verificação, selecione a agenda de backup para a qual deseja executar a operação de verificação e insira o caminho e os argumentos do prescritor ou postscript que deseja executar antes ou depois da operação de verificação, respetivamente.
10. Revise o resumo e clique em **Finish**.

Crie grupos de recursos e anexe políticas de backup Oracle

Um grupo de recursos é o contentor ao qual você deve adicionar recursos que deseja fazer backup e proteger.

Um grupo de recursos permite fazer 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 tarefa de proteção de dados que deseja executar.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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	Introduza um nome para o grupo de recursos.
Tags	Insira um ou mais rótulos que o ajudarão a pesquisar posteriormente o grupo de recursos.

Para este campo…	Faça isso…
Use o formato de nome personalizado para cópia Snapshot	Marque essa caixa de seleção e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.
Destino do ficheiro de registo de arquivo	Especifique os destinos dos ficheiros de registo de arquivo.

4. Na página recursos, selecione um nome de host na lista suspensa **Host** e o tipo de recurso na lista suspensa **Resource Type**.
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 agendas, clique em + para a política que deseja configurar.
   c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação 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 o agendamento de verificação e clique em * + .
   c. Selecione **Executar verificação após cópia de segurança** 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 **Finish**.

Faça backup de bancos de dados Oracle em execução no Azure NetApp Files

Se um recurso ainda não fizer parte de qualquer grupo de recursos, você poderá fazer backup do recurso na página recursos.

Passos

1. No painel de navegação esquerdo, selecione **Resources** 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 **Use o formato de nome personalizado para cópia Snapshot** e insira um formato de nome personalizado que você deseja usar para o nome da captura Instantânea.
4. Na página políticas, execute as seguintes etapas:
   a. Selecione uma ou mais políticas na lista suspensa.
   b. Selecione + * * na coluna Configurar agendas para a política para a qual você deseja configurar um agendamento.

c. Na caixa de diálogo Adicionar agendas para política *policy_name*, configure a programação e selecione **OK**.

5. Na página Verificação, execute as seguintes etapas:
   a. Selecione o servidor de verificação.
   b. Selecione a política para a qual pretende configurar o seu agendamento de verificação e, em seguida, clique em * * + .
   c. Selecione **Executar verificação após cópia de segurança** 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 **Finish**.
8. Selecione **fazer uma cópia de segurança 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 deseja usar para backup.
   b. Clique em **Backup**.
10. Monitorize o progresso da operação clicando em **Monitor** > **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 **Resources** 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 deseja usar para backup.
   b. Selecione **Backup**.
5. Monitorize 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 o seu sistema de arquivos ativo e, em seguida, recuperar o banco de dados.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 a base de dados ou o grupo de recursos na lista.
4. Na exibição Gerenciar cópias, selecione **backups** no sistema de armazenamento primário.
5. Selecione a cópia de segurança na tabela e, em seguida, clique em * .
6. Na página Restaurar escopo, execute as seguintes tarefas:
   a. Selecione RAC se tiver selecionado um backup de um banco de dados no ambiente RAC.
   b. Execute as seguintes ações:
      i. Selecione **todos os dados** se desejar restaurar apenas os arquivos do banco de dados.
      ii. Selecione **tablespaces** se você quiser restaurar apenas as tablespaces.
      iii. Selecione **Refazer arquivos de log** se quiser restaurar os arquivos de log refazer dos bancos de dados de espera do Data Guard ou do ative Data Guard.
      iv. Selecione **bancos de dados conetáveis** e especifique as PDBs que você deseja restaurar.
      v. Selecione * espaços de tabela de base de dados Pluggable (PDB)* e especifique o PDB e os espaços de tabela desse PDB que você deseja restaurar.
      vi. Selecione **Restaurar o banco de dados para o mesmo host onde o backup foi criado** se você quiser restaurar o banco de dados para o mesmo servidor SQL onde os backups são feitos.
      vii. Selecione **Restaurar o banco de dados para um host alternativo** se você quiser que o banco de dados seja restaurado para um servidor SQL diferente no mesmo ou em um host diferente onde os backups são feitos.
      viii. Selecione **altere o estado do banco de dados, se necessário, para restaurar e recuperar** 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 você quiser executar a restauração no local nos cenários em que novos arquivos de dados são adicionados após o backup ou quando LUNs são adicionados, excluídos ou recriados a um grupo de discos LVM.
7. Na página âmbito de recuperação, selecione uma das seguintes opções:
   a. Selecione **todos os Logs** se quiser recuperar para a última transação.
   b. Selecione **Until SCN (System Change Number)** 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 registo de arquivo externo** se pretender especificar a localização dos ficheiros de registo de arquivo externo.
8. Na página Pré-operações e Pós-operações, 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 **Finish**.
11. Monitorize o progresso da operação clicando em **Monitor** > **trabalhos**.

Restaure e recupere espaços de tablespaces usando recuperação ponto no tempo

Você pode restaurar um subconjunto de espaços de tablespaces que foram corrompidos ou descartados sem afetar os outros espaços de tablespaces no banco de dados. O SnapCenter usa o RMAN para executar a recuperação pontual (PITR) dos espaços das tabelas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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. No modo de exibição Gerenciar cópias, selecione **backups** no sistema de armazenamento.

   Se o backup não estiver catalogado, selecione o backup e clique em **Catálogo**.

5. Selecione a cópia de segurança catalogada e, em seguida, clique em * .
6. Na página Restaurar escopo, execute as seguintes tarefas:
   a. Selecione **RAC** se tiver selecionado um backup de um banco de dados no ambiente RAC.
   b. Selecione **tablespaces** se você quiser restaurar apenas as tablespaces.
   c. Selecione **altere o estado do banco de dados, se necessário, para restaurar e recuperar** para alterar o estado do banco de dados para o estado necessário para executar operações de restauração e recuperação.
7. Na página âmbito de recuperação, selecione uma das seguintes opções:
   a. Selecione **Until SCN (System Change Number)** 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-operações e Pós-operações, 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 **Finish**.
11. Monitorize o processo de restauro utilizando a página **Monitor** > **trabalhos**.

Restaurar e recuperar banco de dados conetável usando recuperação pontual

Você pode restaurar e recuperar um banco de dados conetável (PDB) que foi corrompido ou descartado sem afetar as outras PDBs no banco de dados de contentores (CDB). O SnapCenter usa o RMAN para executar a recuperação pontual (PITR) do PDB.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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. No modo de exibição Gerenciar cópias, selecione **backups** no sistema de armazenamento.

   Se o backup não estiver catalogado, selecione o backup e clique em **Catálogo**.

5. Selecione a cópia de segurança catalogada e, em seguida, clique em * .

6. Na página Restaurar escopo, execute as seguintes tarefas:
   a. Selecione **RAC** se tiver selecionado um backup de um banco de dados no ambiente RAC.
   b. Dependendo se você deseja restaurar o PDB ou espaços de tabela em um PDB, execute uma das ações:
      - Selecione **bancos de dados conetáveis (PDBs)** se você quiser restaurar um PDB.
      - Selecione * espaços de tabela de base de dados Pluggable (PDB)* se quiser restaurar espaços de tabela em um PDB.
7. Na página âmbito de recuperação, selecione uma das seguintes opções:
   a. Selecione **Until SCN (System Change Number)** 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-operações e Pós-operações, 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 **Finish**.
11. Monitorize o processo de restauro utilizando a página **Monitor** > **trabalhos**.

Clone 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. Os clones criados são clones espessos e são criados no pool de capacidade pai.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 a base de dados.
4. Na página de exibição Gerenciar cópias, selecione o backup no sistema de storage primário.
5. Selecione a cópia de segurança de dados e, em seguida, clique em * .
6. Na página Nome, selecione se deseja clonar um banco de dados (CDB ou não CDB) ou clonar um banco de dados conetável (PDB).
7. Na página localizações, especifique os detalhes necessários.

   Se os volumes do ANF do banco de dados Oracle estiverem configurados em um pool de CAPACIDADE DE QOS manual, especifique a QOS para os volumes clonados.

   Se A QOS para os volumes clonados não for especificada, a QOS do volume de origem será usada. Se o pool de capacidade DE QOS automático for usado, o valor DE QOS especificado será ignorado.

8. Na página credenciais, execute um dos seguintes procedimentos:
   a. Para o nome da credencial para o usuário do sys, selecione a credencial a ser usada para definir a senha do usuário do sys do banco de dados clone.
   b. Para o nome da credencial da instância ASM, selecione **nenhum** se a autenticação do sistema operacional estiver ativada para conexão com a instância ASM no host clone.

Caso contrário, selecione a credencial Oracle ASM configurada com um usuário "sys" ou um usuário com privilégio "sysasm" aplicável ao host clone.

9. Na página Pre-Ops, especifique o caminho e os argumentos dos prescripts e na seção Configurações de parâmetros de banco de dados, modifique os valores dos parâmetros de 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 **Until Cancel**, o SnapCenter executa a recuperação montando o backup de log mais recente com a sequência ininterrupta de logs de arquivamento após esse backup de dados que foi selecionado para clonagem.
    b. Se você selecionar **Data e hora**, o SnapCenter recupera o banco de dados até uma data e hora especificadas.
    c. Se você selecionar **até SCN**, o SnapCenter recupera o banco de dados até um SCN especificado.
    d. Se você selecionar **especificar locais de log de arquivo externo**, o SnapCenter identifica e monta o número ideal de backups de log com base na SCN especificada ou na data e hora selecionadas.
    e. Por padrão, a caixa de seleção **Create new DBID** está selecionada para gerar um número único (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 com o catálogo RMAN externo onde o banco de dados de origem já está registrado, a operação falha.

    f. Marque a caixa de seleção **Create tempfile for temporary tablespace** se quiser criar um tempfile para o espaço de tabela temporário padrão do banco de dados clonado.
    g. Em **Digite entradas sql para aplicar quando o clone for criado**, adicione as entradas sql que você deseja aplicar quando o clone for criado.
    h. Em **Digite scripts para serem executados após a operação clone**, especifique o caminho e os argumentos do postscript que você deseja executar após a operação clone.
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 **Finish**.
13. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Clone um banco de dados conetável

Você pode clonar um banco de dados conetável (PDB) para um CDB diferente ou mesmo destino no mesmo host ou host alternativo. Você também pode recuperar o PDB clonado para uma SCN ou data e hora desejadas.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 no sistema de storage primário.
5. Selecione a cópia de segurança e, em seguida, clique em *.

6. Na página Nome, selecione **Clonar PDB** e especifique os outros detalhes.
7. Na página localizações, especifique os detalhes necessários.
8. Na página Pre-Ops, especifique o caminho e os argumentos dos prescripts e na seção Configurações de parâmetros de banco de dados, modifique os valores dos parâmetros de banco de dados pré-preenchidos que são usados para inicializar o banco de dados.
9. Na página Pós-operações, **Until Cancel** é selecionado por padrão para executar a recuperação do banco de dados clonado.
    a. Se você selecionar **Until Cancel**, o SnapCenter executa a recuperação montando o backup de log mais recente com a sequência ininterrupta de logs de arquivamento após esse backup de dados que foi selecionado para clonagem.
    b. Se você selecionar **Data e hora**, o SnapCenter recupera o banco de dados até uma data e hora especificadas.
    c. Se você selecionar **especificar locais de log de arquivo externo**, o SnapCenter identifica e monta o número ideal de backups de log com base na SCN especificada ou na data e hora selecionadas.
    d. Por padrão, a caixa de seleção **Create new DBID** está selecionada para gerar um número único (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 com o catálogo RMAN externo onde o banco de dados de origem já está registrado, a operação falha.

    e. Marque a caixa de seleção **Create tempfile for temporary tablespace** se quiser criar um tempfile para o espaço de tabela temporário padrão do banco de dados clonado.
    f. Em **Digite entradas sql para aplicar quando o clone for criado**, adicione as entradas sql que você deseja aplicar quando o clone for criado.
    g. Em **Digite scripts para serem executados após a operação clone**, especifique o caminho e os argumentos do postscript que você deseja executar após a operação clone.
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 **Finish**.
12. Monitorize o progresso da operação selecionando **Monitor** > **trabalhos**.

Gerencie o servidor SnapCenter e os plug-ins

Visualização do painel

Visão geral do painel de instrumentos

No painel de navegação esquerdo do SnapCenter, o painel oferece uma primeira olhada na integridade do sistema, incluindo atividades recentes de trabalhos, alertas, resumo de proteção, eficiência e uso de armazenamento, status de trabalhos do SnapCenter (backup, clonagem, restauração), status de configuração para hosts autônomos e de cluster do Windows, número de máquinas virtuais de armazenamento (SVMs) gerenciadas pelo SnapCenter e capacidade de licença.

As informações exibidas na exibição Painel de controle dependem da função atribuída ao usuário que está conetado no SnapCenter atualmente. Alguns conteúdos poderão não ser apresentados se o utilizador não tiver permissão para visualizar essas informações.

Em muitos casos, você pode ver mais informações sobre um display passando o Mouse em **i**. Em alguns casos, as informações nos relatórios de dashboard estão vinculadas a informações de origem detalhadas em páginas de GUI do SnapCenter, como recursos, Monitor e relatórios.

Atividades de trabalho recentes

O mosaico atividades de trabalho recentes exibe a atividade de trabalho mais recente de qualquer tarefa de backup, restauração e clonagem a que você tenha acesso. Os trabalhos neste visor têm um dos seguintes estados: Concluído, Aviso, Falha, execução, fila e cancelado.

Passar o Mouse sobre um trabalho fornece mais informações. Pode visualizar informações adicionais do trabalho clicando num número de trabalho específico, que o redireciona para a página Monitor. A partir daí, você pode obter detalhes do trabalho ou informações de log e gerar um relatório específico para esse trabalho.

Clique em **See All** (Ver tudo) para ver um histórico de todos os trabalhos do SnapCenter.

Alertas

O bloco Alertas exibe os mais recentes alertas críticos e de aviso não resolvidos para os hosts e o servidor SnapCenter.

A contagem total de alertas de categoria crítico e de aviso é apresentada na parte superior do visor. Clicar nos totais críticos ou de aviso redireciona-o 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 do ecrã redireciona-o para a página Alertas para obter uma lista de todos os alertas.

Resumo de proteção mais recente

O último bloco Resumo de proteção fornece o status de proteção para todas as entidades às quais você tem acesso. Por padrão, o visor é definido para fornecer o status de todos os plug-ins. As informações de status são fornecidas para recursos com backup no storage primário como snapshots e para storage secundário

usando as tecnologias SnapMirror e SnapVault. A disponibilidade das informações de status de proteção para storage secundário é baseada no tipo de plug-in selecionado.

Se você estiver usando uma política de proteção de cofre-espelho, os contadores do resumo de proteção serão exibidos no gráfico de resumo do SnapVault e não no gráfico 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 todas as atividades de armazenamento primário e secundário para o plug-in especificado.

Os relatórios sobre storage secundário se aplicam somente ao SnapVault; os relatórios do SnapMirror não são compatíveis.

O SAP HANA fornece informações de status de proteção para storage primário e secundário para snapshots. Somente o status de proteção de storage primário está disponível para backups baseados em arquivos.

Estado de proteçãoão	Storage primário	Storage secundário
Falha	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 não conseguiram transferir para um destino secundário.
Bem-sucedido	Contagem de entidades em um grupo de recursos, onde o Grupo de recursos foi feito backup 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 que não foram feitas cópias de segurança.	Contagem de entidades que fazem parte de um ou mais grupos de recursos que não estão configurados para que os backups sejam 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 servidor SnapCenter 4,2 e uma versão anterior do plug-in (anterior a 4,2) para criar backups, o bloco **Resumo de proteção mais recente** não exibirá o status de proteção SnapMirror desses backups.

Trabalhos

O bloco tarefas fornece um resumo das tarefas de backup, restauração e clone às quais você tem acesso. Você pode personalizar o período de tempo para qualquer relatório usando o menu suspenso. As opções de

período de tempo são fixadas nas últimas 24 horas, nos últimos 7 dias e nos últimos 30 dias. O relatório padrão mostra os trabalhos de proteção de dados executados durante os últimos 7 dias.

As informações de tarefa de backup, restauração e clone são exibidas nos gráficos donut. Clicar em uma fatia de rosca redireciona você para a página Monitor com filtros de tarefa pré-aplicados à seleção.

Estado do trabalho	Descrição
Falha	Contagem de trabalhos que falharam.
Aviso	Contagem de trabalhos que sofreram um erro.
Bem-sucedido	Contagem de trabalhos que foram concluídos com sucesso.
Em execução	Contagem de trabalhos que estão em execução no momento.

Armazenamento

O bloco armazenamento exibe o armazenamento primário e secundário consumido por tarefas de proteção durante um período de 90 dias, mostra graficamente as tendências de consumo e calcula as economias de armazenamento primário. As informações de armazenamento são atualizadas uma vez a cada 24 horas às 12 da manhã

O total de consumo do dia, que compreende o número total de backups disponíveis no SnapCenter e o tamanho ocupado por esses backups, será exibido na parte superior do visor. Um backup pode ter vários snapshots associados a ele e a contagem refletirá o mesmo. Isso é aplicável a instantâneos primários e secundários. Por exemplo, você criou backups 10, dos quais 2 são excluídos devido à retenção de backup baseada em política e o backup 1 é explicitamente excluído por você. Assim, uma contagem de 7 backups será exibida juntamente com o tamanho ocupado por esses 7 backups.

O fator de economia de storage para storage primário é a taxa de capacidade lógica (economia de clones e snapshots, além de storage consumido) para a capacidade física do storage primário. Um gráfico de barras ilustra a economia de armazenamento.

O gráfico de linha traça separadamente o consumo de storage primário e secundário diariamente durante um período contínuo de 90 dias. Passar o Mouse sobre os gráficos fornece resultados detalhados dia a dia.

Se você usar o servidor SnapCenter 4,2 e uma versão anterior do plug-in (anterior a 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 de status consolidadas para todos os hosts de cluster autônomos ativos e do Windows 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 adjacente aos hosts redireciona você para a seção hosts gerenciados na página hosts. A partir daí, você pode obter informações detalhadas para um host selecionado.

Além disso, este visor mostra a soma de SVMs ONTAP independentes e SVMs ONTAP de cluster que o SnapCenter está gerenciando e a que você tem acesso. Clicar no número adjacente ao SVM redireciona você para a página sistemas de storage. 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. As mensagens de status são fornecidas para cada estado.

Estado da configuração	Descrição
Atualização obrigatória	Contagem de hosts que estão executando plug-ins não suportados e que 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-ins instalado	Contagem de hosts que são adicionados com êxito, mas os plug-ins precisam ser instalados ou a instalação dos plug-ins falhou.
Suspenso	Contagem de hosts cujas programações estão suspensas e estão em manutenção.
Parado	Contagem de hosts que estão ativos, mas os serviços de plug-in não estão em execução.
Host para baixo	Contagem de hosts que estão inativos ou não alcançáveis.
Upgrade 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.
Configure o diretório de log	Contagem de hosts onde o diretório de log tem que ser configurado para SCSQL fazer backup de log de transações.
Configurar plug-ins VMware	Contagem de hosts nos quais o plug-in do SnapCenter para VMware vSphere precisa ser adicionado.
Desconhecido	Contagem de hosts que foram registrados, mas a instalação ainda não foi acionada.

Estado da configuração	Descrição
Em execução	Contagem de hosts que estão ativos e plug-ins estão 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 em que a instalação do plug-in ou a desinstalação estão em andamento.

Como visualizar informações no painel de instrumentos

No painel de navegação esquerdo do SnapCenter, você pode exibir vários painéis ou telas do Painel, juntamente com os detalhes do sistema associados. O número de visores disponíveis no Painel de instrumentos 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 **Dashboard**.
2. Clique nas áreas ativas em cada visor 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 a partir do painel de controle

Você pode solicitar relatórios sobre tarefas de backup, restauração e clone na página Painel de controle. Isso é útil se você quiser identificar o número total de trabalhos bem-sucedidos ou com falha em seu ambiente SnapCenter.

Passos

1. No painel de navegação esquerdo, clique em **Dashboard**
2. Localize o bloco de tarefas no Painel de instrumentos e selecione **Backup**, **Restore** ou **Clone**.
3. Utilizando o menu pendente, selecione o período de tempo para o qual pretende obter informações sobre trabalhos: 24 horas, 7 dias ou 30 dias.

   Os sistemas exibem um gráfico de rosca cobrindo os dados.

4. Clique no corte de rosca que representa as informações do trabalho para o qual deseja um relatório.

   Quando você clica no gráfico de rosca, você é 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 de páginas Monitor, clique em um trabalho específico para selecioná-lo.
6. Na parte superior da página Monitor, clique em **relatórios**.

Resultado

O relatório apresenta informações apenas para o trabalho selecionado. Pode rever o relatório ou transferi-lo para o seu sistema local.

Solicite relatórios sobre o status da proteção a partir do painel de controle

Você pode solicitar detalhes de proteção para recursos gerenciados por plug-ins específicos usando o Dashboard. Somente backups de dados são considerados para o resumo da proteção de dados.

Passos

1. No painel de navegação esquerdo, clique em **Dashboard**.
2. Localize o mosaico Resumo de proteção mais recente no Painel e use o menu suspenso para selecionar um plug-in.

   O Dashboard exibe um gráfico de rosca para os recursos que fazem backup no storage primário e, se aplicável ao plug-in, um gráfico de rosca para os recursos que fazem backup no storage secundário.

   Os relatórios de proteção de dados estão disponíveis apenas para tipos específicos de plug-ins. Especificar **todos os plug-ins** não é suportado.

3. Clique na fatia de rosca que representa o status para o qual você deseja um relatório.

   Quando você clica no gráfico de rosca, você é redirecionado da página Painel para os relatórios e, em seguida, para a página Plug-in. O relatório exibe somente o status do plug-in selecionado. Pode rever o relatório ou transferi-lo para o seu sistema local.

   O redirecionamento para a página relatórios para o gráfico donut do SnapMirror e o backup SAP HANA baseado em arquivos não é suportado.

Gerenciar RBAC

O SnapCenter permite modificar funções, usuários e grupos.

Modificar uma função

É possível modificar uma função 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 feito login como a função "SnapCenterAdmin".

Não é possível 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. Na página Detalhes da função altere as permissões ou desmarque os membros conforme necessário.
5. Selecione **todos os membros desta função podem ver objetos de outros membros** para permitir que outros membros da função vejam recursos como volumes e hosts depois que eles atualizarem a lista de recursos.

   Desmarque essa opção se você não quiser que os membros dessa função vejam objetos aos quais outros membros são atribuídos.

   Quando essa opção está ativada, a atribuição de acesso aos usuários a objetos ou recursos não é necessária se os usuários pertencerem à mesma função que o usuário que criou os objetos ou recursos.

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 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 (grupos de iniciadores), gerenciar sessões iSCSI e migrar dados.

Você pode executar essas tarefas…	Para Microsoft Exchange Server	Para Microsoft SQL Server	Para Microsoft Windows	Para o banco de dados Oracle	Para banco de dados SAP HANA	Para plug-ins compatíveis com NetApp	Para DB2	Para PostgreSQL	Para MySQL
Adicione hosts e instale o pacote plug-in	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Atualize as informações do ESXi para um host	Não	Sim	Não	Não	Não	Não	Não	Não	Não
Suspenda a programações e coloque hosts no 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
Remova os hosts do SnapCenter	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Inicie os serviços de plug-in	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Você pode executar essas tarefas…	Para Microsoft Exchange Server	Para Microsoft SQL Server	Para Microsoft Windows	Para o banco de dados Oracle	Para banco de dados SAP HANA	Para plug-ins compatíveis com NetApp	Para DB2	Para PostgreSQL	Para MySQL
Provisionar discos	Não	Não	Sim	Não	Não	Não	Não	Não	Não
Gerenciar compartilhamentos SMB	Não	Não	Sim	Não	Não	Não	Não	Não	Não
Gerir iGroups	Não	Não	Sim	Não	Não	Não	Não	Não	Não
Gerir sessões iSCSI	Não	Não	Sim	Não	Não	Não	Não	Não	Não

Atualize as informações da máquina virtual

Você deve atualizar as informações da máquina virtual quando as credenciais do VMware vCenter forem alteradas ou o banco de dados ou o host do sistema de arquivos forem reiniciados. A atualização das informações da máquina virtual no SnapCenter inicia a comunicação com o VMware vSphere vCenter e obtém credenciais do vCenter.

Os discos baseados em RDM são gerenciados pelo plug-in SnapCenter para Microsoft Windows, que é instalado no host do banco de dados. Para gerenciar RDMs, o plug-in do SnapCenter 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 deseja atualizar.
4. Clique em **Atualizar VM**.

Modificar hosts de plug-in

Depois de instalar um plug-in, você pode modificar os detalhes do host do plug-in, se necessário. Você pode modificar credenciais, caminho de instalação, plug-ins, detalhes do diretório de log para o plug-in do SnapCenter para Microsoft SQL Server, conta de serviço gerenciado de grupo (gMSA) e porta do plug-in.

Certifique-se de que a versão do plug-in é a mesma da versão do servidor SnapCenter.

Sobre esta tarefa

- Você pode modificar uma porta de plug-in somente depois que o plug-in for instalado.

  Não é possível modificar a porta do plug-in enquanto as operações de atualização estão 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 alterar a porta de um dos componentes, a operação falha e a porta antiga é mantida para todos os componentes.

    Se a porta foi alterada para todos os componentes, mas um dos componentes não consegue iniciar com a nova porta, então 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 falha (com uma mensagem de erro apropriada) e a porta antiga é mantida para ambos os plug-ins.

  - Em uma configuração em cluster, se o SnapCenter não alterar a porta do plug-in que é instalado em um dos nós, a operação falha e a porta antiga é mantida para todos os nós.

    Por exemplo, se o plug-in estiver 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 gMSA, você pode modificar nas janelas **mais Opções**. Quando os plug-ins são instalados sem gMSA, você pode especificar a conta 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 para o qual você deseja modificar e modificar qualquer um dos campos.

   Apenas um campo pode ser modificado de cada vez.

4. Clique em **Enviar**.

Resultado

O host é validado e adicionado ao servidor SnapCenter.

Inicie ou reinicie os serviços de plug-in

A inicialização dos serviços de plug-in do SnapCenter permite que você inicie os serviços se eles não estiverem sendo executados ou reiniciá-los se estiverem em execução. Poderá querer reiniciar os serviços após a manutenção ter sido efetuada.

Certifique-se de que não estão a ser executados trabalhos 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 deseja iniciar.
4. Clique e clique em **Start Service** (Iniciar serviço) ou **Restart Service** (Reiniciar serviço).

   Você pode iniciar ou reiniciar o serviço de vários hosts simultaneamente.

Suspender programações para manutenção do host

Quando você quiser impedir que o host execute qualquer tarefa agendada do SnapCenter, você pode colocar seu host no modo de manutenção. Você deve fazer isso antes de atualizar os plug-ins ou se estiver executando tarefas de manutenção em hosts.

Não é possível suspender as programações em um host que está inativo porque o SnapCenter não pode 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 e, em seguida, clique em **Suspend Schedule** para colocar o host para esse plug-in no modo de manutenção.

   Você pode suspender a programação de vários hosts simultaneamente.

   Você não precisa parar o serviço de plug-in primeiro. O serviço de plug-in pode estar em um estado em execução ou parado.

Resultado

Depois de suspender as programações no host, a página hosts gerenciados mostra **suspenso** no campo de status geral do host.

Depois de concluir a manutenção do host, você pode tirar o host do modo de manutenção clicando em **Ativar agendamento**. Você pode ativar a programação de vários hosts simultaneamente.

Operações suportadas a partir da página recursos

Você pode descobrir recursos e executar operações de proteção de dados na página recursos. As operações que você pode executar diferem com base no plug-in que você está usando para gerenciar seus recursos.

Na página recursos, você pode executar as seguintes tarefas:

Você pode executar essas tarefas…	Para Microsoft Exchange Server	Para Microsoft SQL Server	Para Microsoft Windows	Para o banco de dados Oracle	Para banco de dados SAP HANA
Determine se os recursos estão disponíveis para backup	Sim	Sim	Sim	Sim	Sim
Faça backup sob demanda de um recurso	Sim	Sim	Sim	Sim	Sim
Restauração a partir de backups	Sim	Sim	Sim	Sim	Sim
Backups de clones	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
Monte backups	Não	Não	Não	Sim	Não
Desmontar backups	Não	Não	Não	Sim	Não
Ver detalhes	Sim	Sim	Sim	Sim	Sim

Gerenciar políticas

Você pode separar políticas de um grupo de recursos ou recursos, modificar, excluir, exibir e copiar.

Modificar políticas

Você pode modificar as opções de replicação, as configurações de retenção de instantâneos, a contagem de tentativas de erro ou as informações de scripts enquanto uma política é anexada a um recurso ou grupo de

recursos. Você pode modificar o tipo de programação (frequência) somente depois de desanexar uma política.

Sobre esta tarefa

Modificar o tipo de agendamento em uma diretiva requer etapas adicionais porque o servidor SnapCenter Registra o tipo de agendamento somente no momento em que a diretiva é anexada a um recurso ou grupo de recursos.

Se você quiser…	Então…
Adicione um tipo de agendamento 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 por hora e você quiser adicionar backups diários também, você 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: Por hora e por dia.
Remover ou alterar um tipo de agendamento	Execute o seguinte: 1. Separe a política de todos os recursos e grupos de recursos que usam essa política. 2. Modifique o tipo de agendamento. 3. Anexe a política novamente a todos os recursos e grupos de recursos. Por exemplo, se uma política especificar backups por hora e você quiser alterá-los para backups diários, primeiro você deve desanexar a política.

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 **Finish**.

Desanexe políticas

Você pode separar políticas de um recurso ou grupo de recursos sempre que não desejar que essas políticas governem a proteção de dados para os 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 **Resources** 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 ao grupo de recursos no restante do assistente e clique em **Finish**.

Eliminar políticas

Se você não precisar mais de políticas, talvez queira excluí-las.

Antes de começar

Você deve separar a política dos grupos de recursos ou recursos se a política 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 grupo de recursos e clicando em **Modificar grupo de recursos** para editar as informações fornecidas durante a criação do grupo de recursos.

  Você pode alterar a programação enquanto modifica o grupo de recursos. No entanto, para alterar o tipo de agendamento, 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 dos backups existentes de sistemas de arquivos SQL, Oracle, Windows, aplicações personalizadas e recursos de banco de dados ou grupos de recursos do banco de dados SAP HANA.

- Crie um clone de um grupo de recursos.

  Esta operação é suportada apenas para grupos de recursos SQL (que contém apenas bancos de dados). É possível configurar um agendamento para clonagem de um grupo de recursos (ciclo de vida do clone).

- Impedir o início de operações agendadas em grupos de recursos.

- Excluir um grupo de recursos.

Parar e retomar as operações em grupos de recursos

Você pode desativar temporariamente as operações agendadas a partir de um grupo de recursos. Mais tarde, quando quiser, você pode ativar essas operações.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 você colocou no modo de manutenção, selecione o grupo de recursos e clique em **produção**.

Eliminar grupos de recursos

Você pode excluir um grupo de recursos se não precisar mais proteger os recursos no grupo de recursos. 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 do grupo de recursos. Opcionalmente, é possível forçar a exclusão de todos os backups, metadados, políticas e snapshots associados ao grupo de recursos.

Passos

1. No painel de navegação esquerdo, clique em **Resources** 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 snapshots 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 backups se quiser fornecer um nome melhor para melhorar a capacidade de pesquisa.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.

2. Na página recursos, selecione o grupo de recursos ou recursos na lista suspensa **Exibir**.
3. Selecione o recurso ou grupo de recursos na lista.

   A página de topologia do grupo de recursos ou recursos é exibida. Se o grupo de recursos ou 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** nos sistemas de armazenamento primário.

   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 será possível renomear esses backups catalogados.

5. Selecione a cópia de segurança e, em seguida, clique em .
6. No campo **Renomear backup como**, insira um novo nome e clique em **OK**.

Eliminar cópias de segurança

Você pode excluir backups se não precisar mais do backup 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, não será possível excluir o backup.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o grupo de recursos ou recursos na lista suspensa **Exibir**.
3. Selecione o recurso ou grupo de recursos na lista.

   A página de topologia do grupo de recursos ou recursos é exibida.

4. Na exibição Gerenciar cópias, selecione **backups** nos sistemas de armazenamento primário.

   Não é possível excluir os backups que estão no sistema de storage secundário.

5. Selecione a cópia de segurança e, em seguida, clique em .

   Se você estiver excluindo um backup de banco de dados SAP HANA, os catálogos associados do SAP HANA do backup também serão excluídos.

   Se o último backup restante for excluído, as entradas de 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 têm backups correspondentes no sistema de armazenamento, use 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.

Remova a proteção

Remover proteção exclui todos os backups e descompacta 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 **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o grupo de recursos ou recursos na lista suspensa **Exibir**.
3. Selecione o recurso ou grupo de recursos na lista.

   A página de topologia do grupo de recursos ou recursos é exibida.

4. Selecione o backup e clique em **Remover proteção**.

Excluir clones

Você pode excluir clones se você achar que eles não são mais necessários.

Sobre esta tarefa

Não é possível excluir clones que atuam como fonte para outros clones.

Por exemplo, se o banco de dados de produção for db1, o banco de dados clone1 será clonado do backup de db1 e, posteriormente, clone1 será protegido. O banco de dados clone2 é clonado a partir do backup de clone1. Se você decidir excluir clone1, primeiro você deve excluir clone2 e, em seguida, excluir clone1.

Passos

1. No painel de navegação esquerdo, clique em **Resources** e selecione o plug-in apropriado na lista.
2. Na página recursos, selecione o recurso ou o 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** nos sistemas de storage 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 excluir o clone.
6. Clique em **OK**.

Depois de terminar

Às vezes, os sistemas de arquivos não são excluídos. Você deve aumentar o valor do parâmetro CLONE_DELAY executando o seguinte comando: `./sccli Set-SmConfigSettings`

> O parâmetro CLONE_DELAY_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.

Depois de modificar o valor do parâmetro, reinicie o serviço SnapCenter Plug-in Loader (SPL).

Monitore trabalhos, horários, eventos e logs

Pode monitorizar o progresso dos trabalhos, obter informações sobre trabalhos agendados e rever eventos e registos a partir da página Monitor.

Monitorizar trabalhos

Você pode exibir informações sobre tarefas de backup, clonagem, restauração e verificação do SnapCenter. Você pode filtrar essa exibição com base na data de início e fim, no tipo de tarefa, no grupo de recursos, na política ou no plug-in do SnapCenter. Você também pode obter detalhes adicionais e arquivos de log para tarefas especificadas.

Você também pode monitorar trabalhos relacionados a operações do SnapMirror e do SnapVault.

> Você pode monitorar apenas os trabalhos que criou e que são relevantes para você, a menos que você tenha atribuído a administração do SnapCenter ou outra função de super usuário.

Pode executar as seguintes tarefas relacionadas com tarefas de monitorização:

- Monitore operações de backup, clonagem, restauração e verificação.
- Exibir detalhes e relatórios do trabalho.
- Parar um trabalho agendado.

Gerir trabalhos de cópia de segurança programados

A partir da versão do SnapCenter 6.0.1, foi introduzido um novo parâmetro **JobConcurrenciyThreshold** que define um limite para o número de tarefas agendadas que podem ser executadas 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 **JobConcurrenciyThreshold** é 0 e está desativado. Você pode ativar atribuindo um valor, se observar a degradação do desempenho durante a janela de backup agendada.

> Se você habilitar **JobConcurrenciyThreshold** para gerenciar tarefas simultâneas, o SnapCenter não permitirá que você controle a ordem dos backups e os backups podem não ser acionados ao mesmo tempo especificado na programação.

Passos

1. Defina o valor do parâmetro *JobConcurrenciThreshold* localizado em *C: Arquivos de programas/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 do SnapCenter clicando em IIS > Sites > SnapCenter > Reiniciar.

Gerenciar trabalhos obsoletos

Os 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, é introduzido um cronograma predefinido para limpar esses trabalhos obsoletos que estão presos por mais de 72 horas. Você pode alterar a frequência de programação editando o parâmetro configurável **CleanUpStaleJobsIntervalHours**.

Você pode ativar a limpeza sob demanda executando a programação de **Monitor** > **horários** > **SnapCenter_StaleJobCleanUp**.

Passos

1. Defina o valor do parâmetro *NetApp_SnapCenter_SnapManager.UI.dll.config*.
2. Recicle o pool de aplicativos do SnapCenter clicando em IIS > pools de aplicativos > SnapCenter > Reiniciar.
3. Reinicie o serviço Web do SnapCenter clicando em IIS > Sites > SnapCenter > Reiniciar.

Monitorar programações

Você pode querer ver as programações atuais para determinar quando a operação é iniciada, quando foi executada pela última vez e quando é executada a seguir. Você também pode determinar o host no qual a operação é executada, juntamente com o grupo de recursos da operação e as informações de política.

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página Monitor, clique em **horários**.
3. Selecione o grupo de recursos e o tipo de agendamento.
4. Veja a lista de operações agendadas.

Monitorar eventos

Você pode exibir 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 exibir eventos para determinar se uma operação como uma operação de backup ou uma operação de restauração está em andamento no momento.

Sobre esta tarefa

Todas as informações do trabalho são apresentadas na página Eventos. Por exemplo, quando uma tarefa de backup é iniciada, um evento "'início de backup'" é exibido. Quando o backup for concluído, um evento de "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 fim, a categoria do evento (como backup, grupo de recursos ou política) e o nível de gravidade e clique em **aplicar**. Alternativamente, insira carateres na caixa pesquisar.
4. Veja a lista de eventos.

Monitorizar registos

Você pode exibir e baixar logs do servidor SnapCenter, logs do agente host do SnapCenter e logs de plug-in. Talvez você queira exibir os logs para ajudar na solução de problemas.

Sobre esta tarefa

Você pode filtrar os logs para mostrar apenas um nível específico de gravidade do log:

- Depurar
- Informações
- Avisar
- Erro
- Fatal

Você também pode obter Registros de nível de tarefa, por exemplo, logs que ajudam a solucionar o motivo de uma falha de tarefa de backup. Para registos de nível de trabalho, utilize a opção **Monitor** > **trabalhos**.

Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página trabalhos, selecione um trabalho e clique em Transferir registos.

   A pasta zipada transferida contém os registos de trabalho e os registos comuns. O nome da pasta zipada contém a ID do trabalho e o tipo de tarefa selecionados.

3. Na página Monitor, clique em **Logs**.
4. Selecione o tipo de log, o host e a instância.

   Se você selecionar o tipo de log como **plugin**, você pode selecionar um host ou plug-in SnapCenter. Você não pode fazer isso se o tipo de log for **Server**.

5. Para filtrar os logs por uma fonte, mensagem ou nível de log específico, clique no ícone de filtro na parte superior do cabeçalho da coluna.

   Para mostrar todos os logs, escolha **maior ou igual a** como `Debug` nível.

6. Clique em **Atualizar**.
7. Ver a lista de registos.
8. Clique em **Download** para baixar os logs.

   A pasta zipada transferida contém os registos de trabalho e os registos comuns. O nome da pasta zipada contém a ID do trabalho e o tipo de tarefa selecionados.

Em configurações grandes para um 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 uma tarefa de failover, execute o cmdlet `Get-SmRepositoryConfig`.

Remover trabalhos e registos do SnapCenter

Você pode remover logs e tarefas de backup, restauração, clone e verificação do SnapCenter. O SnapCenter armazena registos de trabalho com êxito e com falha indefinidamente, a menos que os remova. Você pode querer removê-los para reabastecer o armazenamento.

Sobre esta tarefa

Não deve haver trabalhos atualmente em operação. Pode remover um trabalho específico fornecendo uma 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, reveja o estado 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*. Em alternativa, pode também consultar o "Guia de referência de 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 cópia de segurança	O Relatório de backup fornece dados gerais sobre as tendências de backup para o seu ambiente SnapCenter, a taxa de sucesso do backup e algumas informações sobre cada backup realizado durante o tempo especificado. Se um backup for excluído, o relatório não exibirá nenhuma informação de status para o backup excluído. O Relatório de Detalhes da cópia de Segurança fornece informações detalhadas sobre uma tarefa de cópia de segurança especificada e lista os recursos com êxito e os que falharam.
Relatório clone	O Relatório de clones fornece dados gerais sobre tendências de clones para o seu ambiente SnapCenter, a taxa de sucesso de clones e algumas informações sobre cada tarefa de clone executada durante o tempo 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 clone e o status da tarefa de tarefa de clone. Se uma tarefa falhar, o Clone Detail Report exibe informações sobre a falha.
Restaurar relatório	O Relatório de restauração fornece informações gerais sobre os trabalhos de restauração. O Relatório de detalhes de restauração fornece detalhes sobre uma tarefa de restauração especificada, incluindo nome do host, nome do backup, início e duração da tarefa e o status de tarefas individuais. Se uma tarefa falhar, o Relatório de detalhes de restauração exibe informações sobre a falha.
Relatório de proteção	Esses relatórios fornecem detalhes de proteção para recursos gerenciados por todas as instâncias de plug-in do 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 não protegidos, recursos que não foram copiados quando o relatório foi gerado, recursos de um grupo de recursos para o qual as operações de backup falharam e status do SnapVault.

Tipo de relatório	Descrição
Relatório programado	Esses relatórios são programados para serem executados periodicamente, como diariamente, semanalmente ou mensalmente. Os relatórios são gerados automaticamente na data e hora especificadas e o relatório é enviado para as respetivas pessoas por e-mail Pode ativar, desativar, modificar ou eliminar as agendas. A programação ativada pode ser executada sob demanda clicando no botão **Executar agora**. O administrador pode executar qualquer programação, mas o relatório gerado conterá dados com base na permissão fornecida pelo usuário que criou a programação. Qualquer outro usuário que não o Administrador poderá ver ou modificar a programação com base em sua permissão. Se todos os membros desta função puderem ver a opção objetos de outros membros estiver selecionada na página Adicionar função, outros membros da função poderão ver e modificar.

Acesse relatórios

Você pode usar o Painel do SnapCenter para obter uma visão geral rápida da integridade do seu sistema. No Dashboard, você pode detalhar 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 em **último Resumo de proteção** gráfico de pizza para ver mais detalhes na página relatórios.
- No painel de navegação esquerdo, clique em **relatórios**.

Filtre seu relatório

Você pode querer filtrar os dados do relatório de acordo com uma variedade de parâmetros, dependendo do nível de detalhes 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 deseja executar o relatório. Se você omitir a data de fim, você recupera todas as informações disponíveis.
4. Filtre as informações do relatório com base em qualquer um dos seguintes critérios:
    - Grupo de recursos
    - Host
    - Política

- Recurso
- Estado
- 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. Também pode imprimir relatórios.

Passos

1. No painel de navegação esquerdo, clique em **relatórios**.
2. Na barra de ferramentas relatórios, execute um dos seguintes procedimentos:
   - Clique no ícone **alternar visualização de impressão** para visualizar um relatório imprimível.
   - Selecione um formato na lista suspensa ícone **Exportar** para exportar um relatório para um formato alternativo.
3. Para imprimir um relatório, clique no ícone **Imprimir**.
4. Para ver um resumo específico do relatório, desloque-se para a secção adequada 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 configure 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 determinado recurso sejam enviadas para você ou para outras pessoas para que você possa monitorar o status dessas atualizações, você pode configurar a opção para enviar por e-mail os relatórios do SnapCenter 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 para o qual você enviará o e-mail, insira o assunto e clique em **Enviar**.

Configure a opção para 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 que você possa monitorar o status dessas atualizações, você pode configurar a opção para enviar por e-mail os relatórios do SnapCenter quando estiver criando 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 **Resources** e selecione o plug-in apropriado na lista.
2. Selecione o tipo de recurso que deseja exibir e clique em **novo Grupo de recursos** ou selecione um grupo de recursos existente e clique em **Modificar** para configurar relatórios de 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. Digite o endereço de onde o e-mail é enviado, o endereço para o qual o e-mail é enviado e o assunto do e-mail.

Gerenciar o repositório do servidor SnapCenter

As informações relacionadas a várias operações realizadas a partir do SnapCenter são armazenadas no repositório de banco de dados do servidor SnapCenter. Você deve criar backups do repositório para proteger o servidor SnapCenter contra perda de dados.

O repositório do servidor SnapCenter 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 SnapCenter.

- Gerenciamento de conexões de máquina virtual de storage (SVM)

  Você deve configurar as credenciais de storage.

- Provisionamento de hosts

  Pelo menos um disco de storage do NetApp deve estar presente no host do repositório do SnapCenter. Se um disco NetApp não estiver presente no host do repositório do 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 iSCSI LUN ou um VMDK em um dos servidores SnapCenter.

Faça backup do repositório do SnapCenter

Fazer backup do repositório do servidor SnapCenter ajuda a protegê-lo da 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 uma agenda de backup para o repositório SnapCenter

Passos

1. Inicie o PowerShell.
2. No host do servidor SnapCenter, 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.

Veja os backups do repositório SnapCenter

Você pode exibir uma lista de backups do repositório de banco de dados do servidor SnapCenter executando o cmdlet *Get-SmRepositoryBackups*.

Os backups do repositório são criados de acordo com a programação especificada no cmdlet *Protect-SmRepository*.

Passos

1. Inicie o PowerShell.
2. No prompt de comando, insira o cmdlet a seguir e forneça credenciais para se conetar ao servidor SnapCenter: *Open-SMConnection*
3. Liste todos os backups de bancos de dados SnapCenter disponíveis usando o cmdlet *Get-SmRepositoryBackups*.

Restaure o repositório de banco de dados do SnapCenter

Você pode restaurar o repositório SnapCenter executando o cmdlet *Restore-SmRepositoryBackup*.

Quando você estiver restaurando o repositório do SnapCenter, outras operações do SnapCenter que estão sendo executadas serão impactadas porque durante a operação de restauração o banco de dados do repositório não está acessível.

Passos

1. Inicie o PowerShell.
2. No prompt de comando, insira o cmdlet a seguir e forneça credenciais para se conetar ao servidor SnapCenter: *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 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 iSCSI LUN. Para VMDK, restaure manualmente o backup a partir de

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 a execução da operação de restauração.

Migrar o repositório SnapCenter

Você pode migrar o repositório de banco de dados do servidor SnapCenter 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 MySQL.

   Normalmente, você pode encontrar o diretório de dados em C: /ProgramData/MySQL/MySQL Server 5,7/Data.

3. Copie o diretório de dados MySQL para o novo local, por exemplo, e:
4. Clique com o botão direito do rato no novo diretório e selecione **Propriedades** > **Segurança** para adicionar a conta do servidor local do Serviço de rede ao novo diretório e, em seguida, atribua o controlo total da conta.
5. Renomeie o diretório original do banco de dados, por exemplo, nsm_copy.
6. A partir de 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 de localização do banco de dados é bem-sucedida, fazendo login no SnapCenter e verificando entradas do repositório, ou fazendo login no utilitário MySQL e conetando-se ao novo repositório.
9. Exclua o diretório original, renomeado, do repositório de banco de dados (nsm_copy).

Redefina a senha do repositório do SnapCenter

A senha do banco de dados do repositório do servidor MySQL é gerada automaticamente durante a instalação do servidor SnapCenter 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 o Privileges do administrador do SnapCenter para redefinir a senha.

Passos

1. Inicie o PowerShell.
2. No prompt de comando, digite o seguinte comando e, em seguida, forneça as credenciais para se conetar ao servidor SnapCenter: *Open-SMConnection*
3. Redefinir a senha do repositório: *Set-SmRepositoryPassword*

   O seguinte comando 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Gerencie recursos de domínios não confiáveis

Além de gerenciar hosts em domínios confiáveis do ative Directory (AD), o SnapCenter também gerencia hosts em vários domínios não confiáveis do AD. Os domínios do AD não confiáveis devem ser registrados no servidor SnapCenter. O SnapCenter oferece suporte a usuários e grupos de vários domínios do AD não confiáveis.

Você pode instalar o servidor SnapCenter em uma máquina que esteja em um domínio ou em um grupo de trabalho. Para instalar o servidor SnapCenter, 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.

Os grupos do ative Directory (AD) que pertencem a domínios não registrados no servidor SnapCenter não são suportados. Embora você possa criar funções do SnapCenter com esses grupos do AD, fazer login no servidor SnapCenter falha com a seguinte mensagem de erro: O usuário que você está tentando fazer login não pertence a nenhuma função. Contacte o seu administrador.

Modifique 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 como 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 em e, em seguida, 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 domínio FQDN não for resolvível, especifique um ou mais endereços IP do controlador de domínio.

5. Clique em **OK**.

Anular o registo de domínios não fidedignos do ative Directory

Você pode cancelar o Registro de um domínio do ative Directory não confiável 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 não for registrado do servidor SnapCenter, os usuários desse domínio não poderão acessar o servidor SnapCenter.
- Se houver ativos associados (hosts, usuários e grupos), após o cancelamento do 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 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 deseja cancelar o Registro.
5. Clique em e, em seguida, clique em **OK**.

Gerencie o sistema de storage

Depois de adicionar o sistema de armazenamento, você pode modificar a configuração e as conexões do sistema de armazenamento ou excluir o sistema de armazenamento.

Modificar a configuração do sistema de storage

Você pode usar o SnapCenter para modificar a configuração do sistema de armazenamento se quiser alterar o nome de usuário, senha, plataforma, porta, protocolo, período de tempo limite, endereço IP preferido ou opções de mensagens.

Sobre esta tarefa

Você pode modificar 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 é exibido várias vezes na lista de conexão de armazenamento, uma vez para cada grupo com permissão para o sistema de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Storage Systems**.
2. Na página sistemas de armazenamento, na lista suspensa **Type**, execute uma das seguintes ações:

Selecione…	Passos…
SVMs ONTAP	Para visualizar todas as máquinas virtuais de storage (SVMs) adicionadas e modificar a configuração necessária da SVM. a. Na página conexões de storage, clique no nome apropriado do SVM. b. Execute uma das seguintes ações: ◦ Se o SVM não fizer parte de qualquer cluster, na página Modificar sistema de armazenamento, modifique as configurações, como nome de usuário, senha, configurações EMS e AutoSupport, plataforma, protocolo, porta, tempo limite e IP preferido. ◦ 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 EMS e AutoSupport, plataforma, protocolo, porta, tempo limite e IP preferido. Depois de modificar o SVM a ser gerenciado de forma independente, se você decidir gerenciá-lo pelo cluster, exclua o SVM e clique em **redescubra**. O SVM será adicionado ao cluster do ONTAP. Quando uma senha do sistema de armazenamento é atualizada na GUI do SnapCenter, você deve reiniciar os serviços SMCore do respetivo plug-in ou do host do servidor porque a senha atualizada não se reflete no SMCore e os trabalhos de backup falharão com um erro de credencial incorreto.

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 Editar ao lado de Nome de usuário e modifique o nome de usuário e a senha. c. Selecione ou limpe as definições do EMS e do AutoSupport. d. Clique em **mais Opções** e modifique outras configurações, como plataforma, protocolo, porta, tempo limite e IP preferido.

3. Clique em **Enviar**.

Elimine o sistema de armazenamento

Você pode usar o SnapCenter para excluir qualquer sistema de storage não utilizado.

Sobre esta tarefa

Pode eliminar ligações de armazenamento para um utilizador 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 é exibido várias vezes na lista de conexão de armazenamento, uma vez para cada grupo com permissão para o sistema de armazenamento.

Quando você está excluindo um sistema de storage, todas as operações que estão sendo executadas nesse sistema de storage falharão.

Passos

1. No painel de navegação esquerdo, clique em **Storage Systems**.
2. Na página sistemas de armazenamento, na lista suspensa **tipo**, selecione **ONTAP SVMs** ou **ONTAP clusters**.
3. Na página conexões de armazenamento, marque a caixa de seleção ao lado do SVM ou o cluster que você deseja excluir.

   Não é possível 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 um SVM for excluído do cluster do ONTAP usando a GUI do ONTAP, na GUI do SnapCenter, clique em **redescobrir** para atualizar a lista SVM.

Gerir a recolha de dados 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 servidor SnapCenter, os pacotes plug-in do SnapCenter instalados, os hosts e informações semelhantes e, em seguida, enviá-los para uma máquina virtual de armazenamento (SVM) ONTAP especificada.

A utilização da CPU do sistema é elevada quando a tarefa de recolha de dados está em curso. A utilização da CPU permanece elevada enquanto a operação estiver a progredir independentemente do tamanho dos dados.

Parar a recolha de dados EMS

A coleta de dados EMS é ativada por padrão e é executada a cada sete dias após a data de instalação. Você pode desativar a coleta de dados a qualquer momento usando o cmdlet *Disable-SmDataCollectionEMS* do PowerShell.

Passos

1. A partir de uma linha de comando do PowerShell, estabeleça uma sessão com o SnapCenter inserindo *Open-SmConnection*.
2. Desative a coleta de dados EMS inserindo *Disable-SmDataCollectionEms*.

Inicie a recolha de dados EMS

A coleta de dados do EMS é ativada por padrão e está programada para ser executada a cada sete dias a partir da data de instalação. Se você a tiver desativado, você poderá iniciar a coleta de dados EMS novamente usando o cmdlet *enable-SmDataCollectionEMS*.

A permissão Data ONTAP event Generate-AutoSupport-log foi concedida ao usuário da máquina virtual de storage (SVM).

Passos

1. A partir de uma linha de comando do PowerShell, estabeleça uma sessão com o SnapCenter inserindo *Open-SmConnection*.
2. Ative a coleta de dados EMS inserindo *enable-SmDataCollectionEMS*.

Alterar o cronograma de coleta de dados do EMS e o 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, digite o cmdlet *Open-SmConnection*.
2. Para alterar o destino de coleta de dados EMS, digite o cmdlet *Set-SmDataCollectionEmsTarget*.
3. Para alterar o cronograma de coleta de dados EMS, digite o cmdlet *Set-SmDataCollectionEmsSchedule*.

Monitorize o estado da recolha de dados EMS

Você pode monitorar o status da sua coleta de dados EMS usando vários cmdlets do PowerShell. Você pode obter informações sobre a programação, o destino da máquina virtual de storage (SVM) e o status.

Passos

1. A partir de uma linha de comando do PowerShell, estabeleça uma sessão com o SnapCenter inserindo *Open-SmConnection*.
2. Recupere informações sobre o cronograma de coleta de dados EMS inserindo *Get-SmDataCollectionEmsSchedule*.
3. Recupere informações sobre o status da coleta de dados EMS inserindo *get-SmDataCollectionEmsStatus*.
4. Recupere informações sobre o destino de coleta de dados 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

Atualize o servidor SnapCenter e os plug-ins

Configure o SnapCenter para verificar se há atualizações disponíveis

A SnapCenter 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 no qual deseja receber informações sobre atualizações disponíveis.

Passos

1. No painel de navegação esquerdo, clique em **Configurações**.
2. Na página **Configurações**, clique em **Software**.

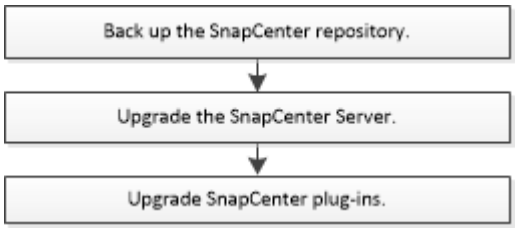
   A página Software disponível exibe os pacotes de plug-in disponíveis, as versões disponíveis e o status da instalação.

3. Clique em **verificar atualizações** para ver se há versões mais recentes de pacotes de plug-in disponíveis.
4. Clique em **Agendar atualizações** para criar uma agenda para especificar o intervalo no qual você deseja receber informações sobre atualizações disponíveis:
   a. Selecione o intervalo em **verificar atualizações**.
   b. Selecione a credencial do Windows Administrador do servidor SnapCenter e clique em **OK**.

Atualizar fluxo de trabalho

Cada versão do SnapCenter contém um servidor SnapCenter atualizado e um pacote de plug-ins. 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 servidor SnapCenter e os pacotes Plug-in.



Caminhos de atualização suportados

Se você estiver na versão do servidor SnapCenter…	Você pode atualizar diretamente o servidor SnapCenter para…	Versões de plug-in suportadas
4,9	5,0	• 4,9 • 5,0
	6,0	• 6,0
5,0	6,0	• 5,0 • 6,0
	6.0.1	• 6.0.1
6,0	6.0.1	• 6,0 • 6.0.1

Por exemplo, se você estiver no SnapCenter versão 4,9 e quiser atualizar para 6,0.1, primeiro você deve atualizar para 5,0 e, em seguida, fazer uma atualização contínua para 6,0.

Para obter informações sobre como atualizar o plug-in do SnapCenter para VMware vSphere, "Atualize o plug-in do SnapCenter para o VMware vSphere" consulte .

Atualize o servidor SnapCenter 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

- O host do servidor SnapCenter deve estar atualizado com as atualizações do Windows, sem reiniciar o sistema pendente.
- Certifique-se de que nenhuma outra operação esteja em execução antes de iniciar a atualização.
- 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, "Faça backup do repositório do SnapCenter"consulte .

- Faça backup de todos os arquivos de configuração modificados do SnapCenter 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 o plug-in do SnapCenter para Microsoft SQL Server, o plug-in do SnapCenter para Microsoft Exchange Server e o plug-in do SnapCenter para Microsoft Windows, é recomendável atualizar o servidor e os hosts do plug-in para a versão 4,7 para a execução do SCRIPT_PATH.

  Para as agendas de backup e verificação existentes com prescripts e pós-scripts ativados na política, as operações de backup continuarão a funcionar após a atualização.

  Na página **Detalhes da tarefa**, uma mensagem de aviso recomenda que o cliente copie os scripts para o SCRIPT_path e edite a política para fornecer um caminho relativo ao SCRIPT_path. Para o trabalho de ciclo de vida do clone, a mensagem de aviso aparece no nível do subtrabalho.

Passos

1. Baixe o pacote de instalação do servidor SnapCenter 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: Arquivos de programas/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 despejo de 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, introduza a palavra-passe.

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. Corrija quaisquer erros antes de continuar. Você pode ignorar os avisos e prosseguir.

   O SnapCenter continuará a usar a senha de banco de dados existente do repositório do servidor MySQL fornecida durante a instalação da versão anterior do servidor SnapCenter.

6. Selecione **Atualizar**.

   Se você selecionar **Cancelar** em qualquer estágio, o SnapCenter interromperá a atualização. O SnapCenter Server não retorna ao seu estado anterior.

   Melhores práticas: Saia e faça login novamente ou abra um novo navegador para acessar a interface do usuário do SnapCenter .

Depois de terminar

- Se o plug-in for instalado usando um usuário sudo, você deve copiar as chaves sha224 disponíveis em *C:/NetApp/SnapCenter para atualizar o arquivo _/etc/sudoers*.
- Você deve executar 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 ao seu estado anterior.
- Depois de atualizar o host do servidor, você também deve atualizar os plug-ins antes de adicionar qualquer sistema de storage.

Atualize o servidor SnapCenter no host Linux

Pode utilizar o ficheiro de instalação do servidor SnapCenter para atualizar o servidor SnapCenter.

Passos

1. Execute uma das ações para atualizar o servidor SnapCenter.

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 registos 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 inteiro diferente de 0 para atualizar o servidor SnapCenter.
Instalação interativa	`./snapcenter-linux-server-(el8/el9/sles15).bin` Você será solicitado a confirmar o upgrade. Introduza qualquer valor diferente de 0 para confirmar a atualização do servidor SnapCenter.

Você deve fazer logout e, em seguida, fazer login no SnapCenter, ou fechar e, em seguida, abrir um novo navegador para acessar a GUI do SnapCenter.

Atualize seus pacotes de plug-in

Os pacotes plug-in são distribuídos como parte da atualização do SnapCenter.

Você não precisa colocar manualmente cada host de plug-in que deseja atualizar para o modo de manutenção, pois o procedimento de atualização coloca seus hosts de plug-in do Windows, Linux ou AIX no modo de manutenção. O modo de manutenção impede que quaisquer trabalhos agendados sejam executados no host do plug-in durante a atualização.

Antes de começar

- Se você é um usuário não-root com acesso às máquinas Linux, você deve atualizar o arquivo */etc/sudoers* com os últimos valores de checksum antes de executar a operação de atualização.
- Por padrão, o SnapCenter deteta JAVA_HOME do ambiente. Se você quiser usar um JAVA_HOME fixo e se você estiver atualizando os plug-ins em um host Linux, você deve adicionar manualmente o parâmetro SKIP_JAVAHOME_UPDATE no arquivo *spl.properties* localizado em */var/opt/SnapCenter/spl/etc/* e definir o valor como TRUE.

O valor de JAVA_HOME é atualizado quando o plug-in é atualizado ou quando o serviço SnapCenter plug-in Loader (SPL) é reiniciado. Antes de atualizar ou reiniciar o SPL, se você adicionar o parâmetro SKIP_JAVAHOME_UPDATE e definir o valor como VERDADEIRO, 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 servidor SnapCenter 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 plug-in do SnapCenter para Microsoft SQL Server, o plug-in do SnapCenter para Microsoft Exchange Server e o plug-in do SnapCenter para Microsoft Windows, é recomendável atualizar o servidor e os hosts do plug-in para a versão mais recente para que o SCRIPT_PATH seja executado.

  Para as agendas de backup e verificação existentes com prescripts e pós-scripts ativados na política, as operações de backup continuarão a funcionar após a atualização.

  Na página **Detalhes da tarefa**, uma mensagem de aviso recomenda que o cliente copie os scripts para o SCRIPT_path e edite a política para fornecer um caminho relativo ao SCRIPT_path. Para o trabalho de ciclo de vida do clone, a mensagem de aviso aparece no nível do subtrabalho.

Passos

1. No painel de navegação à esquerda, clique em **hosts** > **hosts gerenciados**.
2. Atualize os hosts executando uma das seguintes tarefas:
   - Se a coluna Estado geral exibir "Atualização disponível" para um dos plug-ins, 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 **Upgrade**.
   - Se você quiser atualizar vários hosts de plug-in, selecione todos os hosts, clique em e clique em **Upgrade** > **OK**.

     Todos os serviços relacionados são reiniciados durante a atualização do plug-in.

     Todos os plug-ins do pacote são selecionados, mas apenas 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 **Add plug-ins** para instalar qualquer novo plug-in.

     Se você não tiver selecionado a caixa de seleção **Ignorar pré-verificações**, o host do plug-in será validado para ver se ele atende aos requisitos para instalar o plug-in. Se os requisitos mínimos não forem atendidos, mensagens de erro ou aviso apropriadas serão exibidas. Depois de corrigir o problema, clique em **Upgrade**.

Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o web.config localizado em C: SnapCenter, ou os arquivos de configuração do NetApp localizados em C: Windows System32 PowerShell v1,0 módulos SnapCenter para modificar os valores padrão. Se o erro estiver relacionado aos parâmetros restantes, você deve corrigir o problema e, em seguida, validar os requisitos novamente.

Atualização técnica

Atualização técnica do host do servidor SnapCenter

Quando o host do servidor SnapCenter requer atualização, você pode instalar a mesma versão do servidor SnapCenter 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 servidor SnapCenter.
   b. (Opcional) Configurar certificados CA e ativar SSL bidirecional. Para obter mais informações, "Configurar certificado CA" consulte e "Configure e ative SSL bidirecional".
   c. (Opcional) Configurar a autenticação multifator. Para obter mais informações, "Ativar a autenticação multifator" consulte .
2. Faça login como usuário Administrador do SnapCenter.
3. Crie um backup do servidor SnapCenter no host antigo usando a API: `/<snapcenter_version>/server/backup` Ou o cmdlet: *New-SmServerBackup*.

   Antes de efetuar a cópia de segurança, suspenda todos os trabalhos agendados e certifique-se de que não estão a ser executados trabalhos.

   Se você quiser restaurar o backup no servidor SnapCenter que está sendo executado em um novo domínio, antes de fazer um backup, adicione o novo usuário de domínio no host SnapCenter antigo e atribua a função de administrador do SnapCenter.

4. Copie o backup do host antigo para o novo host.
5. Restaure o backup do servidor SnapCenter no novo host usando a API: `/<snapcenter_version>/server/restore` Ou o cmdlet: *Restore-SmServerBackup*.

   Restore atualizará o novo URL do servidor SnapCenter em todos os hosts por padrão. Se você quiser ignorar 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 um dos hosts do plug-in e adicione a entrada *etc/host* para o novo IP no formato <New 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 servidor SnpCenter que está sendo executado em um novo domínio e se você quiser continuar usando os usuários antigos do domínio, você deve Registrar o domínio antigo no novo servidor SnapCenter.

Se você tiver atualizado manualmente o arquivo web.config no antigo host 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 ignorou a atualização do URL do servidor SnapCenter ou qualquer um do host esteve inativo durante o processo de restauração, atualize o novo nome do servidor em todos os hosts ou hosts especificados gerenciados pelo SnapCenter usando a API: `/<snapcenter_version>/server/configureurl` Ou o cmdlet: *Set-SmServerConfig*.
7. Ative os trabalhos agendados em todos os hosts a partir do novo servidor SnapCenter.

Atualização técnica de um nó no cluster F5

Você pode fazer a 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, faça outro nó do cluster como ativo e, em seguida, remova o nó.

Para obter informações sobre como adicionar um nó ao cluster F5, "Configurar servidores SnapCenter para alta disponibilidade usando o F5" consulte .

Se o url do cluster F5 mudar, o url pode ser atualizado em todos os hosts usando a API: `/<snapcenter_version>/server/configureurl` Ou o cmdlet: *Set-SmServerConfig*.

Desativação do antigo host do servidor SnapCenter

Você pode remover o antigo host do servidor SnapCenter depois de verificar se o novo servidor SnapCenter está funcionando e todos os hosts de plug-in podem se comunicar com o novo host do servidor SnapCenter.

Reverter para o antigo host do servidor SnapCenter

Em caso de problemas, você pode trazer de volta o antigo host do servidor SnapCenter atualizando o URL do servidor SnapCenter em todos os hosts usando a API: `/<snapcenter_version>/server/configureurl` Ou o cmdlet: *Set-SmServerConfig*.

Recuperação de desastres

Recuperação de desastres de 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 que tem uma cópia de segurança do servidor SnapCenter antigo.

Passos

1. Implante o novo host e execute as seguintes tarefas:
   a. Instale a mesma versão do servidor SnapCenter.
   b. Configure os certificados de CA e habilite o SSL bidirecional. Para obter mais informações, "Configurar certificado CA" consulte e "Configure e ative SSL bidirecional".
2. Copie o backup antigo do servidor SnapCenter para o novo host.
3. Faça login como usuário Administrador do SnapCenter.

4. Restaure o backup do servidor SnapCenter no novo host usando a API: `/<snapcenter_version>/server/restore` Ou o cmdlet: *Restore-SmServerBackup*.

   Restore atualizará o novo URL do servidor SnapCenter em todos os hosts por padrão. Se você quiser ignorar 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 um dos hosts do plug-in e adicione a entrada *etc/host* para o novo IP no formato <New 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 ignorou a atualização do URL ou qualquer um do host esteve inativo durante o processo de restauração, atualize o novo nome do servidor em todos os hosts ou hosts especificados 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 que tem uma cópia de segurança do servidor SnapCenter antigo.

Passos

1. Implante o novo host e execute as seguintes tarefas:
   a. Instale a mesma versão do servidor SnapCenter.
   b. Configure os certificados de CA e habilite o SSL bidirecional. Para obter mais informações, "Configurar certificado CA" consulte e "Configure e ative SSL bidirecional".
2. Copie o backup antigo do servidor SnapCenter para o novo host.
3. Faça login como usuário Administrador do SnapCenter.
4. Restaure o backup do servidor SnapCenter no novo host usando a API: `/<snapcenter_version>/server/restore` Ou o cmdlet: *Restore-SmServerBackup*.

   Restore atualizará o novo URL do servidor SnapCenter em todos os hosts por padrão. Se você quiser ignorar 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 um dos hosts do plug-in e adicione a entrada *etc/host* para o novo IP no formato <New 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 ignorou a atualização do URL ou qualquer um do host esteve inativo durante o processo de

restauração, atualize o novo nome do servidor em todos os hosts ou hosts especificados gerenciados pelo SnapCenter usando a API: `/<snapcenter_version>/server/configureurl` Ou o cmdlet: *Set-SmServerConfig*.

6. Converta o host autônomo para o cluster F5.

   Para obter informações sobre como configurar o F5, "Configurar servidores SnapCenter para alta disponibilidade usando o F5" consulte .

Informações relacionadas

Para obter informações sobre as APIs, você precisa acessar a página Swagger. "Como acessar APIs REST usando a página da Web da API Swagger"Consulte .

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 de cmdlet do software SnapCenter".

Atualização técnica dos hosts de plug-in do SnapCenter

Quando os hosts do plug-in do SnapCenter precisarem ser atualizados, você deve mover os recursos do host antigo para o novo host. 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 cmdlet, que levará o nome de host antigo e o novo nome de host como entrada, comparar os recursos por nome e revincular os objetos de recursos correspondentes do host antigo para o novo host. 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 novo.

  Depois de verificar os recursos correspondentes, você deve definir o parâmetro *IsDryRun* como Falso 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 apenas para 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 host. Se for uma instância padrão, use *default_instance* como nome da instância.

A atualização técnica é suportada para os seguintes plug-ins do SnapCenter:

- Plug-in do SnapCenter para Microsoft SQL Server
  - Se os bancos de dados SQL estiverem protegidos no nível da instância e como parte da atualização técnica do host, somente os recursos parciais serão movidos para o novo host, a proteção existente no nível da instância será convertida para a 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 técnica no host1, o agendamento ou os detalhes de verificação não serão migrados e continuarão a ser executados no

host1. Se você tiver que modificar, então você deve alterá-lo manualmente nos respetivos hosts.

- Se você estiver usando a configuração FCI (instâncias de cluster de failover SQL), poderá realizar a atualização técnica adicionando o novo nó ao cluster FCI e atualizando o host de plug-in no SnapCenter.
- Se você estiver usando a configuração do SQL Availability Group (AG), a atualização técnica não será necessária. Você pode adicionar o novo nó ao AG e atualizar o host no SnapCenter.

- Plug-in do SnapCenter para Windows
- Plug-in SnapCenter para banco de dados Oracle

  Se você estiver usando a configuração do RAC (Real Application Cluster), poderá realizar a atualização técnica adicionando o novo nó ao cluster RAC e atualizando o host do plug-in no SnapCenter.

- Plug-in do SnapCenter para banco de dados SAP HANA

Os casos de uso suportados são:

- Migração de recursos de um host para outro host.
- Migração de recursos de vários hosts para um ou menos hosts.
- Migração de recursos de um host para vários hosts.

Os cenários suportados são:

- Novo anfitrião tem um nome diferente do antigo anfitrião
- O host existente foi renomeado

Antes de começar

Como este fluxo de trabalho modifica os dados no repositório SnapCenter, recomenda-se fazer backup do repositório SnapCenter. No caso de quaisquer problemas de dados, o repositório SnapCenter pode ser revertido para o estado antigo usando o backup.

Para obter mais informações, "Faça backup do repositório do SnapCenter" consulte .

Passos

1. Implante o novo host e instale o aplicativo.
2. Suspenda os horários 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 storage.
      - 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 respetivo armazenamento deve ser montado no novo host.
   b. Verifique a compatibilidade se houver uma alteração na versão do aplicativo.
   c. Somente para o host de plug-in Oracle, certifique-se de que os UIDs e GIDs da 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 host"
- "Como migrar o banco de dados Oracle do host antigo para o novo host"
- "Como criar um banco de dados SAP HANA para um novo host"

4. Adicione o novo host ao SnapCenter.
5. Verifique se todos os recursos são descobertos.
6. Execute a API de atualização do host: `/<snapcenter_version>/techrefresh/host` Ou o cmdlet: *Invoke-SmTechRefreshHost*.

   A execução a seco é ativada por padrão e os recursos correspondentes a serem vinculados são identificados. Você pode verificar os recursos executando a API: '/jobs/ jobid' ou o cmdlet *get-SmJobSummaryReport*.

   Se você migrou os recursos de vários hosts, execute a API ou o cmdlet para todos os hosts. Se o caminho de unidade ou montagem no novo host não for o mesmo que o antigo host, as seguintes operações de restauração falharão:

   - A restauração no 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 da etapa 1 para todos os hosts.

   Você pode executar a API ou o cmdlet no mesmo host várias vezes, ele será revinculado somente se houver um novo recurso identificado.

7. (Opcional) Remova o host antigo ou hosts do SnapCenter.

Informações relacionadas

Para obter informações sobre as APIs , você precisa acessar a página Swagger. "Como acessar APIs REST usando a página da Web da API Swagger"Consulte .

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 de cmdlet do software SnapCenter".

Atualização técnica do sistema de storage

Quando o storage é atualizado pela tecnologia, os dados são migrados para um novo storage e os hosts de aplicativos são montados com um novo storage. O fluxo de trabalho de backup do SnapCenter identifica o novo storage e cria o snapshot se o novo storage for registrado no SnapCenter.

É possível executar a restauração, a montagem e a clonagem nos novos backups criados após a atualização do storage. No entanto, essas operações falharão quando executadas nos backups que foram criados antes da atualização de armazenamento, pois os backups têm os detalhes de armazenamento antigos. Você deve executar a API de atualização técnica de armazenamento ou cmdlet para atualizar os backups antigos no SnapCenter com os novos detalhes de armazenamento.

A atualização técnica é suportada para os seguintes plug-ins do SnapCenter:

- Plug-in do SnapCenter para Microsoft SQL Server
- Plug-in do SnapCenter para Windows
- Plug-in SnapCenter para banco de dados Oracle
- Plug-in do SnapCenter para banco de dados SAP HANA
- Plug-in do SnapCenter para Microsoft Exchange Server

Os casos de uso suportados são:

- Atualização do storage primário

  A atualização técnica de storage é suportada para substituir o storage primário por um novo storage. Não é possível converter o storage secundário existente em um storage primário.

- Atualização do storage secundário

Os outros cenários suportados são:

- Alteração de nome do SVM
- Alteração do nome do volume

Atualize os backups do armazenamento primário

Quando o armazenamento for atualizado pela tecnologia, você deve executar a API ou cmdlet de atualização técnica de armazenamento para atualizar os backups antigos no SnapCenter com os novos detalhes de armazenamento.

Antes de começar

Como este fluxo de trabalho modifica os dados no repositório SnapCenter, recomenda-se fazer backup do repositório SnapCenter. No caso de quaisquer problemas de dados, o repositório SnapCenter pode ser revertido para o estado antigo usando o backup.

Para obter mais informações, "Faça backup do repositório do SnapCenter" consulte .

Passos

1. Migre os dados do armazenamento antigo para o novo armazenamento.

   Para obter informações sobre como migrar, consulte:

   - "Como migrar os dados para um novo storage"
   - "Como posso copiar um volume e preservar todas as cópias Snapshot?"
2. Coloque o host no modo de manutenção.
3. Monte o novo armazenamento nos respetivos hosts e abra os bancos de dados.

   O novo armazenamento deve ser conetado ao host da mesma maneira que antes. Por exemplo, se ele foi conetado como SAN, ele precisa ser conetado como SAN.

   O novo armazenamento precisa ser montado na mesma unidade ou caminho que o do armazenamento antigo.

4. Verifique se todos os recursos estão ativos e em execução.
5. Adicione o novo armazenamento no SnapCenter.

   Garanta que você tenha um nome exclusivo da SVM nos clusters no SnapCenter. Se você estiver usando o mesmo nome do SVM no novo storage e se todos os volumes do SVM puderem ser migrados antes de executar a atualização de storage, é recomendável excluir o SVM no cluster antigo e redescobrir o cluster antigo no SnapCenter, que removerá o SVM do cache.

6. Coloque o host no modo de produção.
7. No SnapCenter, crie um backup dos recursos cujo storage é migrado. Um novo backup é necessário para que o SnapCenter identifique o espaço físico do storage mais recente e será usado para atualizar os metadados de backups antigos existentes.

   Sempre que um novo LUN for conetado 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 único como novo recurso. Durante a atualização técnica de armazenamento quando o LUN de um novo armazenamento é anexado ao host com a mesma letra ou caminho de unidade, a descoberta do sistema de arquivos do Windows no SnapCenter marcará o recurso existente como excluído, mesmo que ele seja montado com a mesma letra ou caminho de unidade e exibirá o novo LUN como novo recurso. Como o recurso é marcado como excluído, ele não será considerado para atualização técnica de armazenamento no SnapCenter e todos os backups do recurso antigo serão perdidos. Quando a atualização de armazenamento acontece, para recursos do sistema de arquivos do Windows, a descoberta de recursos não deve ser realizada antes de executar a API de atualização de armazenamento ou cmdlet.

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 ativada, o backup mais recente após a atualização de armazenamento deve ter detalhes do armazenamento secundário.

   a. Se você estiver usando a configuração FCI (SQL failover Cluster Instances), os backups serão mantidos no nível do cluster. Você deve fornecer o nome do cluster como entrada para atualização técnica de armazenamento.
   b. Se você estiver usando a configuração do SQL Availability Group (AG), os backups serão mantidos no nível do nó. Você deve fornecer o nome do nó como entrada para atualização técnica de storage.
   c. Se você estiver usando a configuração do Oracle Real Application clusters (RAC), poderá executar a atualização técnica de storage em qualquer nó.

      O atributo *IsDryRun* é definido como true por padrão. Ele identificará os recursos para os quais o armazenamento é atualizado. Você pode exibir 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 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 storage que está sendo migrado tiver metadados clone 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 armazenamento primário, execute a seguinte API: `/<snapcenter_version>/hosts/primarybackupsexistencecheck` Ou o cmdlet *Invoke-SmPrimaryBackupsExistenceCheck*.

    Isso executará a verificação de existência de snapshot no novo armazenamento primário e marcará os respetivos backups não disponíveis para qualquer operação no SnapCenter.

Atualize os backups do armazenamento secundário

Quando o armazenamento for atualizado pela tecnologia, você deve executar a API ou cmdlet de atualização técnica de armazenamento para atualizar os backups antigos no SnapCenter com os novos detalhes de armazenamento.

Antes de começar

Como este fluxo de trabalho modifica os dados no repositório SnapCenter, recomenda-se fazer backup do repositório SnapCenter. No caso de quaisquer problemas de dados, o repositório SnapCenter pode ser revertido para o estado antigo usando o backup.

Para obter mais informações, "Faça backup do repositório do SnapCenter" consulte .

Passos

1. Migre os dados do armazenamento antigo para o novo armazenamento.

    Para obter informações sobre como migrar, consulte:

    - "Como migrar os dados para um novo storage"
    - "Como posso copiar um volume e preservar todas as cópias Snapshot?"
2. Estabeleça a relação SnapMirror entre o storage primário e o novo storage secundário e verifique se o estado da relação está bom.
3. No SnapCenter, crie um backup dos recursos cujo storage é migrado.

    Um novo backup é necessário para que o SnapCenter identifique o espaço físico do storage mais recente e será usado para atualizar os metadados de backups antigos existentes.

    > Deve aguardar até que esta operação esteja concluída. Se você avançar para a próxima etapa antes da conclusão, o SnapCenter perderá completamente os metadados secundários antigos do snapshot.

4. Depois de criar com êxito 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 de armazenamento secundário dos backups mais antigos no host fornecido.

Se você quiser executar isso em nível de recurso, clique em **Atualizar** para cada recurso para atualizar os metadados de armazenamento secundário.

5. Depois de atualizar com êxito os backups mais antigos, você pode quebrar o relacionamento antigo de storage secundário com o primário.

Desinstale o servidor SnapCenter e os plug-ins

Desinstalar pacotes de plug-in do 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 host do servidor SnapCenter ou usando a opção Windows **Desinstalar um programa** localmente em qualquer host.

Antes de remover um host do servidor SnapCenter, você deve concluir os pré-requisitos.

- Você deve fazer login como administrador.
- Você deve garantir que os trabalhos de descoberta não estejam sendo executados 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 falha.
- 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 o controle de acesso baseado em função

- Você deve ter feito login usando uma função RBAC que tenha permissões de leitura, exclusão do host, instalação, desinstalação do plug-in e exclusão de objetos.

  Os objetos podem ser clone, backup, grupo de recursos, sistema de storage etc.

- 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 storage (para clones) que deseja excluir.
- Você deve ter feito login no SnapCenter como um usuário do RBAC.

Pré-requisitos para remover um host com clones criados a partir da operação do ciclo de vida do clone

- Você deve ter criado tarefas de clone usando o gerenciamento do ciclo de vida do clone para bancos de dados SQL.
- Você deve ter criado uma função RBAC com clone de leitura e exclusão, leitura e exclusão de recursos, leitura e exclusão de grupos de recursos, leitura e exclusão de armazenamento, provisionamento de leitura e exclusão, montagem, desmontagem, instalação e desinstalação de plug-ins, permissões de 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 plug-in do SnapCenter para Microsoft SQL Server, às credenciais, ao grupo de recursos do ciclo de vida de clone e ao sistema de storage.
- Você deve ter feito login no SnapCenter como um usuário do RBAC.

Remova um host

Quando o servidor SnapCenter remove um host, ele primeiro remove o backup, clones, tarefas de clone, grupos de recursos e 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, todas as programações associadas também são removidas.
- 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*. Em alternativa, pode também consultar "Guia de referência de 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 deseja remover e clique em **Remover**.
4. Para clusters do Oracle RAC, para remover o software SnapCenter 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 desinstalar e reinstalar os plug-ins do host em um cluster, os recursos do cluster não são detetados automaticamente. Selecione o nome do host do cluster e clique em **Atualizar recursos** para descobrir automaticamente os recursos do cluster.

Desinstale os plug-ins usando a GUI do SnapCenter

Quando você decidir que não precisa mais de um plug-in individual ou de um pacote de plug-in, você pode desinstalá-lo usando a interface SnapCenter.

Antes de começar

- Você deve ter removido os grupos de recursos para o pacote de plug-in que você está desinstalando.
- Você deve ter desanexado as políticas associadas aos grupos de recursos para o pacote de plug-in que você está desinstalando.

Sobre esta tarefa

Você pode desinstalar um plug-in individual. Por exemplo, talvez seja necessário desinstalar o plug-in do SnapCenter para o Microsoft SQL Server porque um host está ficando sem recursos e deseja mover esse plug-in para um host mais poderoso. Você também pode desinstalar todo um pacote de plug-in. Por exemplo, talvez seja necessário desinstalar o pacote de plug-ins do SnapCenter para Linux, que inclui o plug-in do SnapCenter para banco de dados Oracle e o plug-in do SnapCenter para UNIX.

- A remoção de um host inclui a desinstalação de todos os plug-ins.

  Quando você remove um host do SnapCenter, o SnapCenter desinstala todos os pacotes de plug-in no host antes de remover o host.

- A GUI do SnapCenter remove plug-ins de um host de cada vez.

  Quando você usa a GUI do SnapCenter, você pode desinstalar plug-ins em apenas um host de cada 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*. Em alternativa, pode também consultar o "Guia de referência de cmdlet do software SnapCenter".

> Desinstalar o pacote de plug-ins do SnapCenter de um host no qual o servidor SnapCenter está instalado danificará a instalação do servidor SnapCenter. Não desinstale o pacote de plug-ins do SnapCenter para Windows, a menos que você tenha certeza de que não precisa mais do servidor SnapCenter.

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 pacote plug-in ou plug-in.
4. Adjacente ao plug-in que você deseja remover, clique em **Remover** > **Enviar**.

Depois de terminar

Você deve esperar 5 minutos antes de reinstalar o plug-in nesse host. Esse período de tempo é suficiente para que a GUI do SnapCenter atualize o status do host gerenciado. A instalação falha se você reinstalar imediatamente o plug-in.

Se você estiver desinstalando o pacote de plug-ins do SnapCenter para Linux, os arquivos de log específicos de desinstalação estão disponíveis em: */custom_location/SnapCenter/log*.

Desinstale os plug-ins do Windows usando o cmdlet PowerShell

Você pode desinstalar plug-ins individuais ou desinstalar pacotes plug-ins de um ou mais hosts usando o cmdlet *Uninstall-SmHostPackage* na interface de linha de comando do host do servidor SnapCenter.

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 servidor SnapCenter, digite: *Open-SMConnection -SMSbaseUrl://SnapCenter_SERVER_NAME/DOMAIN_NAME* comando e 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 de cmdlet do software SnapCenter".

Desinstale os plug-ins localmente em um host

Você pode desinstalar os plug-ins do SnapCenter localmente em um host se não conseguir acessar o host do servidor SnapCenter.

Sobre esta tarefa

A melhor prática 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 servidor SnapCenter. Esses procedimentos ajudam o servidor SnapCenter a se manter atualizado com quaisquer alterações.

No entanto, você pode ter uma necessidade rara de desinstalar plug-ins localmente. Por exemplo, você pode ter executado uma tarefa de desinstalação do servidor SnapCenter, mas a tarefa falhou, ou você desinstalou o servidor SnapCenter e os 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, tarefas agendadas e metadados de backup.

Não tente desinstalar o pacote de plug-ins do SnapCenter localmente a partir do painel de controle. Você deve usar a GUI do SnapCenter para garantir que o plug-in do SnapCenter para Microsoft Windows esteja 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 do SnapCenter ou o pacote de plug-in que deseja desinstalar e clique em **Desinstalar**.

   O Windows desinstala todos os plug-ins no pacote selecionado.

Desinstale o pacote de plug-ins para Linux ou AIX usando CLI

Você pode desinstalar o pacote de plug-ins do SnapCenter para Linux ou o pacote de plug-ins do SnapCenter para AIX usando a interface de linha de comando.

Antes de começar

- Certifique-se de que eliminou os trabalhos agendados
- Certifique-se de que todos os trabalhos em execução estão concluídos.

Passo

Execute */custom_location/NetApp/SnapCenter/spl/installation/plugins/uninstall* para desinstalar.

Desinstale o servidor SnapCenter no host Windows

Se você não deseja mais usar o servidor SnapCenter para gerenciar tarefas de proteção de dados, você pode desinstalar o servidor SnapCenter usando o Painel de Controle de programas e recursos no host do servidor SnapCenter. Desinstalar o servidor SnapCenter remove todos os seus componentes.

Antes de começar

- Certifique-se de que tem pelo menos 2 GB de espaço livre na unidade onde o servidor SnapCenter está instalado.
- Certifique-se de que o domínio no qual o servidor SnapCenter está instalado não foi removido.

  Se você remover o domínio onde o servidor SnapCenter foi instalado e tentar desinstalar, a operação falhará.

- Você deve ter feito backup do banco de dados do repositório porque o banco de dados do repositório será limpo e desinstalado.

Passos

1. No host do servidor SnapCenter, navegue até o Painel de controle.
2. Certifique-se de que está na vista **Categoria**.
3. Em programas, clique em **Desinstalar um programa**.

   Abre-se a janela programas e funcionalidades.

4. Selecione servidor NetApp SnapCenter e clique em **Desinstalar**.

   A partir do SnapCenter 4,2, quando você desinstalar o servidor SnapCenter, todos os componentes, incluindo o banco de dados do repositório do servidor MySQL é desinstalado.

   - Remover o nó NLB de um cluster NLB requer que você reinicie o host do servidor SnapCenter. Se você não reiniciar o host, poderá ocorrer uma falha se tentar reinstalar o servidor SnapCenter.
   - Você deve desinstalar manualmente o .NET Framework que não é removido durante a desinstalação.

Desinstale o servidor SnapCenter no host Linux

Se você não deseja mais usar o servidor SnapCenter para gerenciar tarefas de proteção de dados, você pode desinstalar o servidor SnapCenter. Desinstalar o servidor SnapCenter remove todos os seus componentes.

Passos

1. Execute uma das ações para desinstalar o servidor SnapCenter.

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` Introduza qualquer valor diferente de 0 na entrada de confirmação para confirmar a desinstalação.

Automatize com o uso de APIS REST

Visão geral das APIs REST

As APIS REST podem ser usadas para executar várias 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 emitir manualmente uma chamada de API.

Os plug-ins compatíveis com APIs REST são:

- Plug-in para Microsoft SQL Server
- Plug-in para banco de dados SAP HANA
- Plug-in para Oracle Database

Como acessar a API REST do SnapCenter nativamente

Você pode acessar a API REST do SnapCenter diretamente usando qualquer linguagem de programação compatível com um CLIENTE REST. As opções de linguagem populares incluem Python, PowerShell e Java.

Base de serviços web REST

Representational State Transfer (REST) é um estilo para a criação de aplicações web distribuídas. Quando aplicada ao design de uma API de serviços da Web, ela estabelece um conjunto de tecnologias e melhores práticas para expor recursos baseados em servidor e gerenciar seus estados. Ele usa protocolos e padrões mainstream para fornecer uma base flexível para o gerenciamento de SnapCenter.

Recursos e representação do Estado

Os recursos são os componentes básicos de um sistema baseado na Web. Ao criar um aplicativo REST de serviços da Web, as tarefas iniciais de design incluem:

Identificação de recursos baseados em sistema ou servidor

Cada sistema usa e mantém recursos. Um recurso pode ser um arquivo, transação comercial, processo ou entidade administrativa. Uma das primeiras tarefas no projeto de um aplicativo baseado 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 de extremidade URI

Todos os recursos REST devem ser definidos e disponibilizados usando um esquema de endereçamento bem definido. Os endpoints onde os recursos estão localizados e identificados usam um URI (Uniform Resource Identifier).

O URI fornece uma estrutura geral para criar um nome exclusivo para cada recurso na rede. O Uniform Resource Locator (URL) é um tipo de URI usado com serviços da Web para identificar e acessar recursos. Os recursos são normalmente expostos em uma estrutura hierárquica semelhante a um diretório de arquivos.

Mensagens HTTP

O Hypertext Transfer Protocol (HTTP) é o protocolo usado pelo cliente e servidor de serviços da Web para trocar mensagens de solicitação e resposta sobre os recursos.

Como parte do projeto de um aplicativo de serviços da Web, os métodos HTTP são mapeados para os recursos e as ações de gerenciamento de estado correspondentes. HTTP está sem estado. Portanto, para associar um conjunto de solicitações e respostas relacionadas como parte de uma transação, informações adicionais devem ser incluídas nos cabeçalhos HTTP carregados 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 da Web de várias maneiras, a opção mais popular é JavaScript Object Notation (JSON).

JSON é um padrão da indústria para representar estruturas de dados simples em texto simples e é usado para transferir informações de estado descrevendo os recursos. A API REST do SnapCenter usa JSON para formatar os dados transportados no corpo de cada solicitação e resposta HTTP.

Caraterísticas operacionais básicas

Embora O REST estabeleça um conjunto comum de tecnologias e práticas recomendadas, os detalhes de cada API podem variar com base nas escolhas de design.

Transação de API de solicitação e resposta

Cada chamada de API REST é executada como uma solicitação HTTP para o sistema servidor SnapCenter que gera uma resposta associada ao cliente. Esse 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 de 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
- Leia

- Atualização
- Eliminar

Para alguns dos recursos, apenas um subconjunto das operações é suportado.

Identificadores de objeto

Cada instância ou objeto de recurso 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 servidor SnapCenter específico.

Depois de emitir uma chamada de API que cria uma nova instância de objeto, um URL com a ID associada é retornado ao chamador no cabeçalho do local da resposta HTTP. Você pode extrair o identificador e usá-lo em chamadas subsequentes quando se refere à instância de recurso.

O conteúdo e a estrutura interna dos identificadores de objeto podem mudar a qualquer momento. Você só deve usar os identificadores 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 de 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, caso se espera 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 tarefa para ancorar a tarefa. O código de status HTTP 202 é retornado ao chamador juntamente com o objeto de tarefa. Você deve recuperar o estado do trabalho para determinar o sucesso ou a falha.

As solicitações que usam os métodos POST e DELETE são projetadas para serem executadas de forma assíncrona se espera 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 servidor SnapCenter e o cliente geralmente é criptografado usando TLS, com base nas configurações do SnapCenter.

Autenticação HTTP

Em um nível HTTP, a autenticação básica é usada para as transações da API. Um cabeçalho HTTP com o nome de usuário e senha em uma cadeia de carateres 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 através 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 finais REST.

Método HTTP	Descrição
OBTER	Recupera propriedades de objeto em uma instância ou coleção de recursos.
POST	Cria uma nova instância de recurso com base na entrada fornecida.
ELIMINAR	Exclui uma instância de recurso existente.
COLOQUE	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, esse cabeçalho deve ser definido como *application/json*.

Aceitar

Esse cabeçalho deve ser definido como *application/json*.

Autorização

A autenticação básica deve ser definida com o nome de usuário e senha codificados como uma string base64.

Corpo do pedido

O conteúdo do corpo da solicitação varia de acordo com a 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:

```
<field>=<query value>
```

Além de uma correspondência exata, outros operadores estão disponíveis para retornar um conjunto de objetos em uma faixa de valores. A API REST do SnapCenter suporta os operadores de filtragem mostrados na tabela abaixo.

Operador	Descrição
.	Igual a.
*	Menos de
>	Superior a.
O que é que eu tenho	Inferior ou igual a
>	Maior ou igual a
ATUALIZAÇÃO	Ou
!	Não é igual a
*	Wildcard ganancioso

Você também pode retornar uma coleção de objetos com base 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 estão definidos são geralmente excluídos de consultas correspondentes.

Solicitando campos de objeto específicos

Por padrão, a emissão de uma chamada de API usando O GET retorna apenas os atributos que identificam exclusivamente o objeto ou objetos. Este conjunto mínimo de campos atua como uma chave para cada objeto e varia de acordo com o tipo de objeto. Você pode selecionar propriedades de objeto adicionais usando o `fields` parâmetro de consulta das seguintes maneiras:

Campos comuns ou padrão

Especifique **campos*** para recuperar os campos de objeto mais comumente usados. Esses campos são normalmente mantidos na memória do servidor local ou requerem pouco processamento para acessar. Estas são as mesmas propriedades retornadas para um objeto depois de usar GET com uma chave de caminho de URL (UUID).

Todos os campos

Especifique **campos ** ** para recuperar todos os campos de objeto, incluindo aqueles que exigem processamento adicional de servidor para acessar.

Seleção de campo personalizada

Use **fields <field_name>** para especificar o campo exato desejado. Ao solicitar vários campos, os valores devem ser separados usando vírgulas sem espaços.

> Como prática recomendada, você deve sempre identificar os campos específicos que deseja. Você só deve recuperar o conjunto de campos comuns ou todos os campos quando necessário. Quais campos são classificados como comuns e retornados usando *fields**, são determinados pelo NetApp com base na análise interna de desempenho. A classificação de um campo pode mudar em versões futuras.

Ordenar 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 de 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 maior número possível de objetos com base em duas restrições. Você pode controlar cada uma dessas restrições usando parâmetros de consulta adicionais na solicitação. A primeira restrição alcançada para uma SOLICITAÇÃO GET específica termina a solicitação e, portanto, limita o número de Registros retornados.

> Se uma solicitação terminar antes de iterar 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 um máximo de 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 do que o máximo em efeito, com base na restrição de tempo relacionada, bem como o número total de objetos no sistema.

Limitar o tempo usado para recuperar os objetos

Por padrão, o SnapCenter retorna o maior número possível de objetos dentro do tempo permitido para a solicitação GET. O tempo limite padrão é de 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 efeito, com base na restrição relacionada ao número de objetos, bem como o número total de objetos no sistema.

Estreitar 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 inteiro em bytes, você pode opcionalmente usar um sufixo como mostrado na tabela a seguir.

Sufixo	Descrição
KB	KB kilobytes (1024 bytes) ou kibibytes
MB	MB megabytes (KB x 1024 bytes) ou megabytes
GB	GB Gigabytes (MB x 1024 bytes) ou gibytes
TB	TB Terabytes (GB x 1024 byes) ou tebibytes
PB	PB petabytes (TB x 1024 byes) ou petabytes

Interpretação de uma resposta API

Cada solicitação de API gera uma resposta de volta 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.
201	Criado um objeto foi criado com sucesso. O cabeçalho de localização na resposta inclui o identificador exclusivo para o objeto.

Código	Descrição
202	Aceite Um trabalho em segundo plano foi iniciado para executar a solicitação, mas ainda não foi concluído.
400	Solicitação incorreta a entrada de solicitação não é reconhecida ou é inadequada.
401	A autenticação de utilizador não autorizado falhou.
403	O acesso proibido é negado devido a um erro de autorização (RBAC).
404	Não encontrado o recurso referido 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 estão incluídos na resposta HTTP gerada pelo SnapCenter.

Localização

Quando um objeto é criado, o cabeçalho do local 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.

Um único objeto

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` a indicação do número de Registros e Registros contendo um array das instâncias do objeto. Por exemplo, você pode recuperar os nós definidos em um cluster específico.

Objeto trabalho

Se uma chamada de API for processada de forma assíncrona, um objeto Job será retornado que ancora a tarefa em segundo plano. Por exemplo, a SOLICITAÇÃO DE 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 de erro é 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 de resposta inclui um objeto JSON vazio.

Erros

Se ocorrer um erro, um objeto de erro é retornado no corpo de resposta.

Formato

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 de erro geral 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. As 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 em falta ou um campo extra foi fornecido.
400	A operação não é suportada.
405	Não é possível encontrar um objeto com o identificador especificado.
403	A permissão para executar a solicitação é negada.
409	O recurso está em uso.

APIs REST compatíveis com servidor SnapCenter 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 de uso adicionais, quando apropriado.

Auth

Você pode usar essa API para fazer login no servidor SnapCenter. Esta API retorna um token de autorização de usuário que é usado para autenticar solicitações subsequentes.

Domínios

Você pode usar APIs para executar operações diferentes.

- Recupere todos os domínios no SnapCenter
- recuperar detalhes de um domínio específico
- registrar ou cancelar o registro de um domínio
- modificar um domínio

Trabalhos

Você pode usar APIs para executar operações diferentes.

- Recupere todos os trabalhos no SnapCenter
- recuperar o status de um trabalho
- cancelar ou parar um trabalho

Definições

Você pode usar APIs para executar operações diferentes.

- registre, modifique ou remova uma credencial
- Exibe as informações de credenciais registradas no servidor SnapCenter
- configure as definições 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 servidor SnapCenter
- Ative ou desative e configure o MFA para o login do servidor SnapCenter
- Crie o arquivo de configuração necessário para configurar o MFA

Hosts

Você pode usar APIs para executar operações diferentes.

- Consultar todos os hosts SnapCenter
- Remova 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
- recupere os detalhes de configuração do plug-in
- configure o host do plug-in
- Recuperar todos os recursos do plug-in para o host Microsoft SQL Server
- Recuperar todos os recursos do plug-in para o host de banco de dados Oracle
- recupere todos os recursos do plug-in para o host de aplicativos personalizados
- Recuperar todos os recursos do plug-in para host SAP HANA
- recupere os plug-ins instalados
- instale plug-ins em um host existente
- atualize o pacote de host
- remova plug-ins de um host existente
- adicione plug-in em um host
- adicionar ou modificar host
- Obtenha a assinatura do host Linux
- Registre a assinatura do host Linux
- coloque o host no modo de manutenção ou produção
- inicie ou reinicie os serviços de plug-in no host
- renomeie um host

Recursos

Você pode usar APIs para executar operações diferentes.

- recuperar todos os recursos
- Recuperar um recurso usando o ID do recurso
- Recuperar todos os recursos do plug-in para o host Microsoft SQL Server
- Recuperar todos os recursos do plug-in para o host de banco de dados Oracle
- recupere todos os recursos do plug-in para o host de aplicativos personalizados
- Recuperar todos os recursos do plug-in para host SAP HANA
- Recuperar um recurso do Microsoft SQL Server usando uma chave
- recuperar um recurso personalizado usando uma chave
- modifique um recurso do plug-in para o host de aplicativos personalizados

- remova um recurso do plug-in para o host de aplicativos personalizados usando uma chave
- Recuperar um recurso do 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 aplicativos Oracle
- Modificar um recurso de volume de aplicativos Oracle
- Remova um recurso de volume de aplicativos Oracle usando uma chave
- Recuperar os detalhes secundários do recurso Oracle
- Faça backup do recurso Microsoft SQL Server usando plug-in para Microsoft SQL Server
- Faça backup do recurso Oracle usando 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
- Configure o banco de dados Oracle
- Restaurar um backup de banco de dados SQL
- Restaurar um backup de banco de dados Oracle
- restaure um backup de aplicativo personalizado
- Criar um recurso do SAP HANA
- proteja um recurso personalizado usando o plug-in para aplicativos personalizados
- Proteja um recurso do Microsoft SQL Server usando o plug-in para Microsoft SQL Server
- Modifique um recurso protegido do Microsoft SQL Server
- Remova a proteção do recurso Microsoft SQL Server
- Proteger um recurso Oracle usando plug-in para banco de dados Oracle
- Modificar um recurso Oracle protegido
- Remova a proteção do recurso Oracle
- clonar um recurso do backup usando o plug-in para aplicação personalizada
- Clonar um volume de aplicações Oracle a partir do backup usando o plug-in para banco de dados Oracle
- Clonar um recurso do Microsoft SQL Server a partir do backup usando o plug-in para Microsoft SQL Server
- Crie um ciclo de vida clone de um recurso do Microsoft SQL Server
- Modifique o ciclo de vida do clone de um recurso do Microsoft SQL Server
- Excluir ciclo de vida de clone de um recurso do Microsoft SQL Server
- Mova um banco de dados existente do Microsoft SQL Server de um disco local para um LUN NetApp
- Crie um arquivo de especificação clone para um banco de dados Oracle
- Inicie 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 clone
- restaura o banco de dados para a réplica secundária e junta o banco de dados de volta ao grupo de disponibilidade

- Criar um recurso de volume de aplicativos Oracle

Backups

Você pode usar APIs para executar operações diferentes.

- recuperar detalhes da cópia de segurança por nome, tipo, plug-in, recurso ou data da cópia de segurança
- recuperar todos os backups
- recuperar detalhes da cópia de segurança
- renomear ou excluir backups
- Montar um backup Oracle
- Desmontar um backup Oracle
- catalogue 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 operações diferentes.

- Crie, exiba, modifique e exclua o arquivo de especificação do clone do banco de dados Oracle
- Exibir hierarquia de clones de banco de dados Oracle
- recuperar detalhes do clone
- recuperar todos os clones
- excluir clones
- Recuperar detalhes do clone por ID
- Inicie um trabalho de atualização de clone sob demanda de um recurso Oracle
- Clonar um recurso Oracle a partir do backup usando o arquivo de especificação clone

Divisão de clones

Você pode usar APIs para executar operações diferentes.

- estime a operação de divisão do clone do recurso clonado
- recuperar o status de uma operação de divisão de clones
- inicie ou pare uma operação de divisão de clones

Grupos de recursos

Você pode usar APIs para executar operações diferentes.

- recuperar detalhes de todos os grupos de recursos
- recuperar o grupo de recursos por nome
- crie um grupo de recursos para plug-in para aplicativos personalizados

- Crie um grupo de recursos para plug-in para Microsoft SQL Server
- Criar um grupo de recursos para plug-in para banco de dados Oracle
- modifique um grupo de recursos para plug-in para aplicativos personalizados
- 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
- Crie, modifique ou exclua o ciclo de vida do clone de um grupo de recursos para plug-in para Microsoft SQL Server
- faça 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 operações diferentes.

- recuperar detalhes da política
- recuperar detalhes da política por nome
- eliminar uma política
- crie uma cópia de uma política existente
- criar ou modificar política para plug-in para aplicação personalizada
- 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 de plug-in para banco de dados SAP HANA

Armazenamento

Você pode usar APIs para executar operações diferentes.

- recuperar todos os compartilhamentos
- 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
- descubra recursos em um cluster de storage
- recuperar recursos em um cluster de armazenamento

Partilhar

Você pode usar APIs para executar operações diferentes.

- recuperar os detalhes de um compartilhamento
- recuperar detalhes de todas as ações

- crie ou exclua um compartilhamento no armazenamento
- recuperar um compartilhamento pelo nome

Plugins

Você pode usar APIs para executar operações diferentes.

- listar todos os plug-ins de um host
- Recuperar um recurso do Microsoft SQL Server usando uma chave
- modifique um recurso personalizado usando uma chave
- remova um recurso personalizado usando uma chave
- Recuperar um recurso do SAP HANA usando uma chave
- Modificar um recurso do SAP HANA usando uma chave
- Remover um recurso do SAP HANA usando uma chave
- Recuperar um recurso Oracle usando uma chave
- Modificar um recurso de volume de aplicativos Oracle usando uma chave
- Remova um recurso de volume de aplicativos Oracle usando uma chave
- Faça backup do recurso Microsoft SQL Server usando plug-in para Microsoft SQL Server e uma chave
- Faça backup do recurso Oracle usando plug-in para banco de dados Oracle e uma chave
- faça backup do recurso de aplicativo personalizado usando o plug-in para aplicativo personalizado e uma chave
- Configurar o banco de dados SAP HANA usando uma chave
- Configure o banco de dados Oracle usando uma chave
- restaure um backup de aplicativo personalizado usando uma chave
- Criar um recurso do SAP HANA
- Criar um recurso de volume de aplicativos Oracle
- proteja um recurso personalizado usando o plug-in para aplicativos personalizados
- Proteja um recurso do Microsoft SQL Server usando o plug-in para Microsoft SQL Server
- Modifique um recurso protegido do Microsoft SQL Server
- Remova a proteção do recurso Microsoft SQL Server
- Proteger um recurso Oracle usando plug-in para banco de dados Oracle
- Modificar um recurso Oracle protegido
- Remova a proteção do recurso Oracle
- clonar um recurso do backup usando o plug-in para aplicação personalizada
- Clonar um volume de aplicações Oracle a partir do backup usando o plug-in para banco de dados Oracle
- Clonar um recurso do Microsoft SQL Server a partir do backup usando o plug-in para Microsoft SQL Server
- Crie um ciclo de vida clone de um recurso do Microsoft SQL Server
- Modifique o ciclo de vida do clone de um recurso do Microsoft SQL Server
- Excluir ciclo de vida de clone de um recurso do Microsoft SQL Server

- Crie um arquivo de especificação clone para um banco de dados Oracle
- Inicie um ciclo de vida do clone sob demanda de um recurso Oracle
- Clonar um recurso Oracle a partir do backup usando o arquivo de especificação clone

Relatórios

Você pode usar APIs para executar operações diferentes.

- recupere relatórios de operações de backup, restauração e clone para os respetivos plug-ins
- adicionar, executar, excluir ou modificar programações
- recuperar dados para os relatórios programados

Alertas

Você pode usar APIs para executar operações diferentes.

- recuperar todos os alertas
- Recuperar alertas por IDs
- Excluir vários alertas ou excluir um alerta por ID

RBAC

Você pode usar APIs para executar operações diferentes.

- recupere detalhes de usuários, grupos e funções
- adicionar ou excluir usuários
- atribuir utilizador à função
- anular a atribuição do utilizador da função
- criar, modificar ou excluir funções
- atribuir grupo a uma função
- anular a atribuição de um grupo de uma função
- adicionar ou excluir grupos
- crie uma cópia de uma função existente
- atribuir ou anular a atribuição de recursos ao utilizador ou grupo

Configuração

Você pode usar APIs para executar operações diferentes.

- ver as definições de configuração
- modifique as definições de configuração

CertificateSettings

Você pode usar APIs para executar operações diferentes.

- Exibir o status do certificado para o servidor SnapCenter ou host de plug-in
- Modifique as configurações de certificado para o servidor SnapCenter ou host de plug-in

Repositório

Você pode usar APIs para executar operações diferentes.

- recupere os backups do repositório
- veja as informações de configuração sobre o repositório
- Proteja e restaure o repositório do SnapCenter
- Desproteger o repositório SnapCenter
- reconstruir e fazer failover no repositório

Versão

Você pode usar essa API para exibir a versão do SnapCenter.

Como acessar APIs REST usando a página da Web da API 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 servidor SnapCenter, bem como emitir manualmente uma chamada de API. Você pode usar APIS REST para ajudar a gerenciar seu servidor SnapCenter ou para executar operações de proteção de dados.

Você deve saber o endereço IP de gerenciamento ou o nome de domínio do servidor SnapCenter no qual deseja executar as APIS REST.

Você não precisa de permissões especiais para executar o cliente API REST. Qualquer usuário pode acessar a página da Web do Swagger. As respetivas permissões nos objetos que são acessados através da API REST são baseadas no usuário que gera o token para fazer login na API REST.

Passos

1. Em um navegador, digite o URL para acessar a página da Web do Swagger no formato _ https:// SnapCenter_IP_address_or_name>: SnapCenter_port>/swagger/_.

   Certifique-se de que o URL da API REST não tem os seguintes carateres: ., % e &.

2. No campo **exploração do Swagger**, se a documentação da API 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 da 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 APIs REST do SnapCenter, poderá usar os

arquivos de log para identificar a causa e resolver o problema. Pode transferir os ficheiros de registo a partir da interface de utilizador do SnapCenter clicando em **Monitor** > **Registos** > **Download**.

Comece a usar a API REST

Você pode começar rapidamente a usar a API REST do SnapCenter. Acessar a API fornece alguma perspetiva antes de começar a usá-la com os processos de fluxo de trabalho mais complexos em uma configuração ao vivo.

Olá mundo

Você pode executar um comando simples em 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 está disponível no seu sistema.
- Endereço IP ou nome de host do servidor SnapCenter
- Nome de usuário e senha de uma conta com autoridade para acessar a API REST do SnapCenter.

> Se suas credenciais incluem carateres especiais, você precisa formatá-los de uma forma aceitável para Curl com base no shell que você está usando. Por exemplo, você pode inserir uma barra invertida antes de cada caractere especial ou envolver toda `username:password` a cadeia em aspas simples.

Passo

Na interface da 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 de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos 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 de terceiros e licenças usadas no software NetApp.

"Aviso para SnapCenter 6,0"

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.